Development of a Theory-Based Ontology of Design-Induced Error

Shin, Injae

Award date:
2009

Awarding institution:
University of Bath

Development of a Theory-based Ontology of Design-Induced Error

In Jae Shin

A thesis submitted for the degree of Doctor of Philosophy

University of Bath

Department of Mechanical Engineering

July 2009

Abstract

The research in this thesis focuses on investigating the possible influence of design of artefacts and systems on human error, and developing means by which the factors contributing to human error related to design can be better understood. The thesis suggests that integration of current theories related to human error and design issues can help designers to pick up design issues from human error cases. The motivation of the research was initiated by the non-existence of a unique human error theory relating design issues and human error. These theories have never been systematically reviewed for their characteristics and relationships. The diversity of theories makes it difficult to identify design issues from human error cases. The premise that a collective model can be constructed with a paradigm is the basis of the research. The expression "design-induced error" in this thesis is used to refer to human error influenced by design.

This thesis proposes a meta-theory of design-induced error to provide an integrated and collective view of related theories by comparing their key characteristics and adopting a paradigm. The thesis then develops an ontology of design-induced error based on the meta-theory. The developed ontology is a reasoning support tool in knowledge-based systems aiming to capture and to recognise design issues in human error cases. The models developed were examined through the analysis of accident reports. The Australian aviation accident report system (AAARS) is the main source for the experiment.

The ontology developed of design-induced error describes concepts and relations that relate to capturing design issues from human error cases. The ontology examines terms in accident documents such as terms indicating human error and the role of design. The software for developing a knowledge model (e.g. PCPACK) enables us to break down documents into concepts and relations in order to pick up relevant terms effectively from documents.

The models developed in this research provide analytical means for designers as well as accident analysts to identify relevant design issues from accident cases or documents.

Acknowledgements

The research presented in this thesis could not have been carried out without the generous and devoted assistance of the following people:

First of all I owe a big debt of gratitude to **Professor Chris McMahon**, my supervisor, because without his extensive supervision and invaluable support throughout the project my work could not have been accomplished.

I would also like to express my deep appreciation to **Dr Jerry Busby**, my co-supervisor, for giving me encouragement and insight on design and human error issues; and also **Dr Ralph Hibberd** for theoretical support with his special knowledge on psychological theories; **Dr Shanghee Kim** for insightful comments on ontology development; **Professor Steve Culley**, my examiner, for his highly useful comments on research methodologies; and **Dr Crispin Hales**, external examiner who encourage me.

I am also grateful to all the members of the Innovative Manufacturing Research Centre (IMRC) in the Mechanical Engineering Department of the University of Bath, including administrative staff, technician, and cleaners in the department, especially Dr Mansur Darlington, Peter Wild, and Dr Mattew Guiess.

Finally, I would like to give my very special thanks to my family for granting me the privilege of pursuing this PhD; both my parents, **Kyungtae Shin** and **Gangae Lee**, and parents in law, **Taesoo Jang** and **Okyoun Park**, for their confidence in me and prayer; my brothers and sister for their supports and encouragement; my wife, **Eunkyoung Jang**, for being my enthusiastic supporter; my son and daughter, **Junghwang** and **Heyjin** for their patient and smiles. Thanks to them, one of my long journey was finished.

My PhD research was primarily funded by Korean Government Scholarships.

Table of Contents

List of Figures

List of Tables

Acronyms

AAIB:	Air Accidents Investigation Branch
ASN:	Aviation Safety Network
AASIR:	Australia Aviation Safety Investigation Report
ATSB:	Australian Transport Safety Bureau
CHA:	Cambridgeshire Health Authority
FMC	Flight Management Computer
GPWS	Ground Proximity Warning System
GEMS	General Error Modelling system
HSE:	Health and Safety Executive
NTSB:	National Transportation Safety Board (USA)
NASA	National Aeronautics and Space Administration (USA)

Chapter 1. Introduction

The purpose of this research is to examine the influence of design on human error (how design affects the performance and cognition of human operators), and to find effective methods to share knowledge taken from human error theories that describe human–system interaction failures (i.e. human error) in terms of the role of design (how to develop analytical tools that help to capture such issues). This thesis proposes a meta-theory of design-induced error in order to provide an integrated and collective view of related theories. The thesis then develops an ontology of design-induced error based on the meta-theory. The developed ontology is a reasoning support tool in knowledge-based systems in order to capture and to recognise design issues in human error cases. The models developed were examined through the analysis of accident reports.

It is said that design is one of the most influential factors in our society. Human error still accounts for a large proportion of all incidents and accidents. The human being is a social creature affected by its environment. Design and humans have relations in using and operating a system. The questions are: How to investigate these relations? What are the adverse effects of design on human operators? These are research questions that are addressed in this thesis.

There are two premises in the research. The first premise investigated in this thesis is that human error can be studied from a perspective that there are different rationalities on design between designers and operators and these differences may lead to human errors, a phenomenon called design-induced error in this thesis. The second premise is that an extended concept of design may be useful to find hidden influences of design on the incidence of human errors.

This thesis addresses these issues with two approaches: a theoretical approach and a knowledge management approach. The first approach focuses on finding an underlying structure in current relevant theories. The latter adopts a technology of knowledge-based systems to pick up relevant issues from accident reports.

In Section 1.1 the significance of the role of design in human–system interaction is presented, and Section 1.2 discusses design and safety. Section 1.3 reviews briefly current human error research issues and then relevant research issues are discussed in Section 1.4. Section 1.5 addresses the research aims and objectives of this research. In Section 1.6 research methodology adopted in the research is presented and Section 1.7 sets out the limitations of the research. Finally Section 1.8 outlines the remaining chapters.

1.1 Significance of the role of design in human- system interaction failures

Engineering design has changed the world. It influences all parts of our lives including social systems (e.g. social cultures in our society) and technical systems (e.g. machinery in chemical plants). The areas and perspectives of engineering design research, as a result, should no longer remain limited in meaning to physical design, such as equipment design. It needs to address the contextual aspect between systems (design) and users (operators).

With the evolutionary growth of modern technologies, the design of artefacts or systems needs to tackle issues related to more delicate and subtle human–system interaction than before. A number of failures have been reported from safety-critical areas (e.g. aviation, manufacturing, or medical service) in our life including fatal accidents (e.g. the Chernobyl nuclear accident). As a result, appropriate models to represent the role of design in human–system interaction failures have been inevitable, particularly for the implicit and indirect effects of design on human cognition and performance that have been more and more prevalent and important in current complex systems.

> We have to design equipment to take full advantage of the capabilities of our personnel and we have to design equipment that will not overload, confuse or degrade personnel performance in achieving mission objectives ... We have to reduce design-induced human error which is so costly a component of accidents and operational failures. We have to plan for the wise and judicious use of the limited personnel and skill levels available to us by optimizing manpower requirements, and through more effective use of automation and expert systems. We have to design with greater efficiency and productivity in order to reduce costs to our services and to our nations.
>
> [Rear-Admiral R. Horne, USN, 1990]

It is said that one of the foundations for change in our society comes from design. As a result of the development of modern design technologies, the world that we inhabit is increasingly a designed world, from highly sophisticated nuclear power plants to everyday life. Therefore, the role of design in safety of our life has been increased more and more. Human users in a system need to adapt to the system. However, there are

inherent discrepancies between humans and systems [Norman, 1998]. Designers have to understand the characteristics of systems as well as that of humans in the system. The importance of the role of design in human–system interaction failures was depicted in the following accident cases.

> On 4 September 2000, a AA aircraft, VH-SKC, departed Perth, Western Australia, at 1009 UTC on a charter flight to Leonora [833 km NE of Perth] with one pilot and seven passengers on board. … However, shortly after the aircraft had climbed through its assigned altitude, the pilot's speech became significantly impaired and he appeared unable to respond to ATS instructions. … No human response of any kind was detected for the remainder of the flight. Five hours after taking off from Perth, the aircraft impacted the ground near Burketown, Queensland, and was destroyed. There were no survivors. … The investigation found that the pilot was correctly licensed, had received the required training, and that there was no evidence to suggest that he was other than medically fit for the flight. The weather presented no hazard to the operation of the aircraft on its planned route. The aircraft's flightpath was consistent with the aircraft being controlled by the autopilot with no human intervention after the aircraft passed position DEBRA. After the aircraft climbed above the assigned altitude of FL250, the speech and breathing patterns of the pilot displayed changes that were consistent with hypoxia, but a rapid or explosive aircraft cabin depressurisation was unlikely to have occurred. … The investigation concluded that while there are several possible reasons for the pilot and passengers being incapacitated, the incapacitation was probably a result of hypobaric hypoxia due to the aircraft being fully or partially unpressurised and their not receiving supplemental oxygen. However, the investigation concluded that an aural warning for high cabin altitude, and setting visual and aural alerts to operate when the cabin pressure altitude exceeds 10,000 ft, may have prevented the accident. [ATSB, ASIR 200003771[1]]

However this was not the first case of this type of error. There was a precursor before the accident. Similar accidents had happened before the tragedy.

[1] ATSB refers to the Australian Transport Safety Bureau and ASIR is acronym of Aviation Safety Investigation Report. ATSB investigates aviation accidents or incidents and publishes ASIR. The number is an occurrence number of an accident investigated by ATSB.

> On 21 June 1999, the BB registered AA aircraft, a flight from Edinburgh, [South Australia], to Oakey, Qld, was conducted as a single-pilot operation. … After take-off, as the aircraft climbed through 10,400 ft, the pilot began the 'climb checklist' actions. While performing these checks he received a tracking change instruction from Air Traffic Control (ATC). The passenger in the co-pilot seat noticed that this appeared to temporarily distract the pilot from the checklist as he attempted to reprogram the global positioning system (GPS). The pilot then completed the checklist. During this, the passenger in the co-pilot's seat saw the pilot reposition the engine bleed air switches from the top to the centre positions. As the aircraft reached the cruise level of FL250, the controller contacted the pilot, indicating that the aircraft was not maintaining the assigned track. The pilot acknowledged this transmission. A short time later the passenger in the co-pilot seat noticed that the pilot was again attempting to program the GPS, and was repeatedly performing the same task. The controller advised the pilot again that the aircraft was still off track, however the pilot did not reply to this transmission. Shortly after this, the pilot lost consciousness. The passenger in the co-pilot seat took control of the aircraft and commenced an emergency descent. … Significant factors of the accident are pointed out in this case. Both bleed air switches were inadvertently selected to ENVIR OFF at about 10,000 ft in the climb. The cockpit warning system did not adequately alert the pilot to the cabin depressurisation. It is likely that the provision of an audible warning device as strongly recommended in CAO 108.26 would have alerted the pilot to the developing pressurisation problem. [ATSB, ASIR 199902928; and see Section 8.2.1, Case 1]

The above accident cases show an example of the importance of the cooperation of human-system interaction in a system, and the significance of the role of design in human-system interaction. These cases also imply that we have to know why operators suffer from following the specifications of a system as designed; and how failure occurs in systems.

During the period this research was conducted there was a tragic aviation accident in Greece, on 14 August 2005 [Aviation Safety Network, 2005]. A Boeing 737 of Helios flight 522 departed Larnaca in Cyprus on a scheduled flight of 1 hour and 23 minutes to Athens. After an intermediate stop there, it was to have continued on to Prague, Czech Republic. The flight having cleared for an en route altitude of FL 340, reportedly notified the Cypriot controllers that they had some problems with the air conditioning system. The 737 entered Greek air space about 10:30, but efforts by air traffic controllers to contact the pilots were futile. Around 11:00, two Greek F-16 fighter planes were scrambled from the Nea Anghialos air base. About half an hour later the F-16's intercepted the airliner. The F-16 pilots reported that they were not able to observe

the captain, while the first officer seemed to be unconscious. The aircraft descended and crashed in mountainous terrain north of Athens resulting in 121 fatalities. The sequence of events in this accident case may be similar to that described in above cases of loss of cabin pressure.

There are different ways of understanding how the human-system interaction failures occur; operator error only or design involvement. If a human-system interaction failure is recognised as one of the design issues, the error can be considered as an engineering failure, i.e. design specification relating to the failures may possibly be developed into preventive measures to contain such failures (a vertical process in Figure 1.1). However, if a human-system interaction failure is not accepted as a design issue but as operator error only, the human-system interaction failure may be developed into an organisational approach (i.e. training problems or procedure issue) (a horizontal process in Figure 1.1). The selection of methods of development depends on the way people understand the role of design in human-system interaction. The concept of design-induced error adopted the in this research is an active interpretation of human–system interaction failure in order for designers to design a credible system.

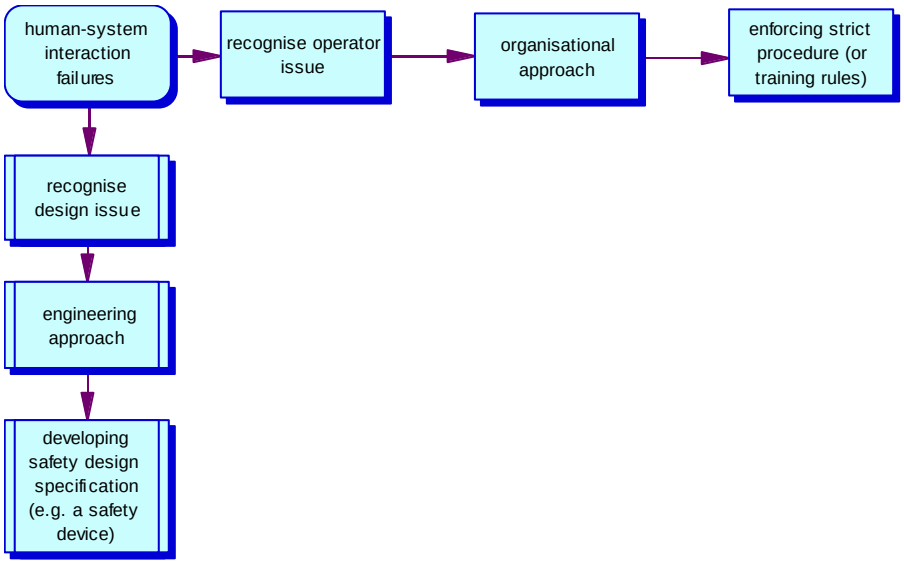


Figure 1.1 Different approaches of human–system interaction failures

Human error is a failure committed by a human operator of a system. A systematic approach to the investigation of accidents emphasises the root causes of the accident, such as a managerial or regulatory body which was responsible for constructing more credible systems (Johnson, 2003; Levenson, 2004). The failures described above may be regarded as human errors and corrective actions will be made at a personal or organisational level e.g. improving training programmes for the operators. As a result,

these approaches may result in a failure to encourage design improvements, and the opportunity to improve systems may be missed.

For example, a forklift is a piece of equipment that is commonly used in many places, such as factories, construction sites, warehouses and even in the services sector, for transporting heavy or bulky goods. Each year about ten thousand workers are injured and hundreds die due to forklift accidents in the USA alone (Bureau of Labor Statistics, US Department of Labor). The major dangers of the equipment are rollover on an uneven road or curve, and impact with people who are behind the vehicle. To solve the problem, health and safety executives have introduced strict regulations since the 1970s. The regulation focuses on the procedures of operation and training of the people who use the equipment. Sets of safety rules restricting human behaviour demand human caution and perception of the dangers involved. The problems of overturning and unintentional backward impacts have not yet been overcome, however. Designers have not yet developed fundamental solutions (i.e. design improvement in the structure and safety measures) for the issue. Safety issues concerning use of the equipment, therefore, are still the same as 30 years ago because human cognition cannot be changed by regulations.

Reason [1997] argued that one of the important root causes or latent conditions is the design of systems. However in most accident reports involving cases of human error, it is not easy to find design issues being addressed. Rather it is easy to emphasise training issues (or procedure issues) of the operator. In order to address the design issue in human–system interaction failures, therefore, the concept of **design-induced error** is introduced

. The concept of design-induced error originated from a review of the literature on design and human error. The purpose of this research is to disseminate the concept in the form of a meta-theory and ontology of design-induced error.

The first and most fundamental reason to deliver the concept of design-induced error is the fact that humans cannot be treated merely as mechanically logical creatures when designing the interaction between human operators and a system. If the designer wants to design a system avoiding design-induced error, she or he must understand human perception and behaviour in relation to the designed system.

Human behaviour is associated with physiological and psychological interaction. Psychological elements consist of cognitive mode and emotional mode [Norman, 2004]. Emotional mode means the fundamental cognitive condition while the cognitive mode refers to logical activity. The emotional mode refers to the underlying reasoning of human performance and behaviour (e.g. selecting what to do), on the contrary, the

cognitive mode is rather logical and conscious. They are related with each other psychologically in the human mind and cannot be separated.

Human decision-making processes are a main factor that rule human performance [Rasmussen, 1986]. They are affected by fundamental cognitive activity (i.e. emotional mode) as well as the logical cognition of humans (i.e. cognitive mode). Designers, however, tend to depend on their logic on a system and ignore the relationship between logical cognition and emotional cognition of human operators when designing a system.

1.2 Design and Safety

Samuel and Weir [2000] described failures as an intrinsic aspect of engineering design. "Engineers are inherently concerned with failure and our vision of success is to develop modelling tools to avoid it. Moreover, by studying failures we develop clear ideas about causal relationships in complex real-life engineering situations, often too difficult to model completely realistically for structural analysis." [p.5].

Petroski [1985] also argued that the history of design is a history of accidents and errors of design and their recovery. Human error has been one of the major concerns of research into system design. Researchers have noted that human error was a causal factor in a large proportion of system failures and accidents [Reason, 1997]. For instance, research on Canadian aviation accidents between 1996 and 2003 showed that nearly 75% of the accidents were attributed to human error as a primary cause [Johnson and Holloway, 2004].

Design contributes to errors and accidents directly and indirectly. Some wrong designs can lead to electrical, mechanical or structural failure of an artefact or system. For example, the specification of a boiler may not describe an appropriate thickness of boiler wall to contain the expected operating pressures. In this case, it may be relatively easy to find the cause of the failures and to remedy the problem, simply through recalculation. However it is not as easy to detect and solve design problems that arise from the specification of designs that lead users to act in a manner that can lead to potentially catastrophic errors in the control of a system. As said in this thesis, the term "design-induced error" will be used for representing design-related human error theories that describe design issues which negatively affect operators' use of the system and which promote errors in operators' performance.

Communication between designers and users is essential in order to avoid the design-induced errors that arise undetected from the design process. Through discourse with

users, designers can gain knowledge of how to reduce or prevent unnecessary errors that arise from the inappropriate design of artefacts and systems. Norman [1993] argued that designers should try to understand users' mental process if they wanted to design more user-friendly artefacts.

However, there are two main problems that make it difficult to engage users in the design process. Firstly, limited finance, space and time can restrict the degree to which users can participate in the design process. Secondly, it is difficult to capture all the relevant problems that arise during typical operations even when there is an opportunity to interact with users. Users possess only limited experience which may not capture all relevant potential failure conditions of the artefact. To compensate for these limitations, researchers have adopted a number of methods for testing artefacts and systems, including usability testing [e.g. Stanton, 2002], and ex-post-facto examination of accidents.

Usability tests have been widely used in the domain of computer software design, and can help to remedy potential problems with the software before it is released onto the market [Wichansky, 2000]. However, due to its time consuming process and its limited applications to static human-machine interface, current usability testing needs further development of theoretical models for understanding interaction and practical tools for engineers and designers [Koubek et al., 2003].

The design process combines philosophies, theories, technologies, methods, and knowledge [Horvath, 2001]. Thinking about safety is one of the important elements in the design process [Cully, 2004]. Human factors, which are a major concern for safety, appear throughout many design areas such as;

- Design Philosophy: What makes the product user-friendly?
- Design Ethnography: Who will use the artefact?
- Design Cognition: How can ambiguity in system displays be removed?
- Design Ergonomics: What makes the system comfortable for the user to use?
- Design Standard: What needs to be done to ensure the artefact or system complies with safety regulations?

It is inevitable that humans will occasionally act erroneously. In response, designers

have tried to mitigate the causes of accidents and their consequences. Sanders and McCormick [1993] describe some well-known principles of safer design, which include:

- *Exclusion designs*: designs that prevent the operator making a specific error.

- *Prevention designs*: designs that make it difficult, but not impossible, for an operator to make a particular error.

- *Fail-safe designs*: designs that mitigate against the consequences of an operator error without necessarily reducing the likelihood of this error.

However, in the evolutionary development of technologies, such as the explosion in the use of computers to manage aspects of complex systems, designers now confront a problem that is distinct from traditional hazards that resulted from moving components, corrosion and structural failure – the problem of error in an operator's cognition about the system. These problems are difficult to catch and deal with because they stem from the minds of the operators and the designers.

Therefore, preventing human error cannot be achieved by simply attempting to produce systems that prescribe rules that the operator should follow, but by design research and development that pays attention to both a psychological and a technical approach in every setting [e.g. Senders, 1993].

It is critical to understand human performance using psychological tools and to create a useful artefact matching with human cognition and performance using technical tools in order to achieve safer design. The increasing use of automation, and computers in particular, which has led to the development of increasingly complex systems such as those used in nuclear power generation, chemical production, or the flight of an aircraft, has been a new challenge for designers because the increase in complexity has provided new ways for the operators to make errors. Experience has shown that these errors can give rise to major accidents [Kletz, 1994; Perrow, 1984]. Perrow [1984] described such an error, and its consequence as a "normal accident" because the error and accident originated from the normal activities of tightly coupled technological systems.

The main problem posed by the introduction of automation is that the greater the operator's exclusion from the control loop of a system, the more the system may need human intervention in critical situations. Bainbridge [1983] referred to this problem as the "Ironies of Automation". In the design of complex systems, we need to take account

a new concepts relating to the interaction between human and artefact, rather than traditional approaches to defending systems, such as defence-in-depth philosophy, which would stipulate the need for ever greater numbers of automatic safety devices.

The study of organisations that successfully manage potentially hazardous technical operations suggests that the success of these organisations did not depend on them merely avoiding risks or errors, but rather on them anticipating and planning for unexpected events and future surprises [Rochlin, 1999]. Designers and researchers support these efforts by generating knowledge about the uses of artefacts and systems, and not just through the use of increasing numbers of safety devices.

Safety in design is not a commodity, but should be a necessary area of study supported by continuous investigation of the interaction between humans and systems. Effective interaction depends on the open flow of information between operators and systems [Vicente and Rasmussen, 1992].

1.3 Human Error Research: need for designers to understand human–system interaction failures

Woods [2000] pointed out that in order to understand and predict human performance with any system in a complex setting, we need to make use of the different languages, i.e. psychological concepts to describe human performance. Woods addressed the reason why designers have to understand human error. The reliability of man–machine interaction is an important issue because the dependence on man–machine interaction has increased in every domain.

The understanding of human error as a behavioural phenomenon, therefore, has become an inherent part of design, especially in safety critical domains such as nuclear power generation, aviation, and off-shore petrochemical production. Rasmussen [1985] argued for the study of human reliability as a primary research area for design, stating that:

> It also seems to be important to realize that the scientific basis for human reliability considerations will not be the study of human error as a separate topic, but the study of normal human behaviour in real work situations and the

> mechanisms involved in adaptation and learning. The findings may very well lead to design of more reliable systems, without improving the basis of quantitative prediction of reliability in the higher-level mental tasks required in new systems.
>
> [Rasmussen, 1985: p.1124].

Hollnagel [1992] clearly defined the purposes of research on human performance as follows:

- To enable specific system changes to be made in response to specific unwanted occurrences, i.e. modifications after the fact (a pragmatic purpose).
- To be able to make better predictions of what will happen under given conditions, in an effort to improve the system design (an engineering purpose, and also an extension of the first purpose).
- To increase knowledge in general about man–machine systems, how they work, and to provide better theories of how they work (a scientific purpose, again extending the previous purpose).

There are different perspectives within the field of human error research. For designers, their primary need is to understand man–machine interaction, a component of human performance control [Neisser, 1976]. To design a credible artefact or system it is necessary to understand the interaction between humans and systems, in which the factors that degrade human performance and the inaccurate execution of plans can be examined and corrected.

1.4 Research issues in design and human–system interaction failures

There are many issues concerning design and human error [Alkov, 1997]. Some fundamental questions posed in this research area are:

- What are the theories concerning relationships between design and human error?

- Why was operator performance incongruent with the designers' expectations about that behaviour at the time of accidents?

- Why designs have failed occasionally and not prevented major accidents even if they were equipped with a number of modern technological systems?

- How can we extract knowledge relevant to designing more credible artefacts and systems from examples of failure and experience of operation?

- How can knowledge-based systems (KBSs) help designers to recognise and reason about design issues in human–system interaction failures?

Additionally, there is ambiguity in the taxonomy used to describe knowledge in the study of human error. For example, the term "human error" itself is ambiguous as the term has three different meanings: the cause of an event or action (e.g. the oil spill was caused by human error); the event or action (e.g. I forgot to check the water level); the consequence of an event or action (e.g. I made the error of putting salt in the coffee) [Hollnagel, 1998]. Therefore, it is important to provide designers with explicit, and usable terminology of design-induced error. Extracting semantic meanings in terms of design-induced error would be helpful for designers in constructing a knowledge base for the design of safer systems.

Although we have to depend on psychological theories to understand human–system interaction failures, many theories appear for the explanation and they exist respectively. In order to recognise design issues in human–system interaction failures more effectively than before, it will be useful if we provide some effective methods to examine and to reason on design issues in human–system interaction failures by combining psychological theories and knowledge engineering techniques.

1.5 Research aims and objectives

The purpose of this thesis presented here is to examine the influence of design on human error, and to find effective methods to share knowledge taken from human error theories that describe human–system interaction failures (i.e. human error) in terms of the role of design. For this purpose the aims of the thesis is to propose a meta-theory of design-induced error, an integrated and collective view on these theories, in order to

present better understanding of how design induces human errors. This thesis then develops an ontology of design-induced error based on the meta-theory in order to make it possible to capture the issues from accident reports. These are the main objectives of the research.

From the aims of this research, the following five objectives are broken down:

1) *To identify issues involved in a design's influences on human error. (Chapter 2)*

2) *To develop an integrated framework taken from related theories that describes relations between design and human error. (Chapter 4)*

3) *To analyse accident cases with the framework developed. (Chapter 5)*

4) *To develop a knowledge model for capturing useful texts in the description of accident documents. (Chapter 7)*

5) *To demonstrate how the developed knowledge model can help to analyse accident cases that include design issues in human errors. (Chapter 8)*

1.6 The research methodology

The research was a combination of human error research and knowledge-based system research. This research generally adopted the methodology discussed by Senders and Moray [1991]. This comprises literature review, logical construction of theories, development of a classification scheme and experiments in accident report systems as the main methodologies of the research as follows.

1) Conduct a literature review on human error and design issues. (Chapter 2)

2) Construct logical relationships between design and human errors. (Chapter 4)

3) Construct a model of design-induced error consisting of related theories. (Chapter 4)

4) Examine accident reports in terms of the design-induced error concept. (Chapter 5)

5) Develop an ontology model using knowledge model development software. (Chapters 6, 7)

6) Apply the model and ontology into real accident cases or documents to illustrate how the model can be used to capture design issues from the cases. (Chapters 5, 8)

The following describes methodologies to fulfil each objective in the research.

The first objective to identify the issues involved in design's influences on human errors was examined through conducting a detailed literature review. This literature review covers the investigation of human error theories relating to design issues. With the human error theories the role of design in complex systems was investigated.

The second objective, to develop a collective model taken from related theories that describe relations between design and human error, was addressed through the examination of underlying structures of related theories. This investigation contained the extended design concepts and an ontological paradigm. The examination of current views on the concept of design-induced error was also conducted. The development of a meta-theory was conducted by adopting a contextual paradigm that represents a collective view on related theories.

The third objective, to analyse accident cases with the framework developed, was addressed through conducting an examination of accident investigation reports of the Australian aviation accident report system as discussed later in Section 3.5, Chapter 5, and Section 7.2.

The fourth objective, to develop a knowledge model for capturing useful texts in the documents describing accidents, was addressed through the investigation of knowledge acquisition and sharing technology, specifically in accident report systems. The development of a knowledge-based ontology of design-induced error that can be used in knowledge management systems was constructed with a computer software program of knowledge model development kits.

The fifth objective, to demonstrate how developed models can help to analyse accident cases that include design issues with human errors, was addressed by examination of the developed meta-theory and the knowledge-based ontology for knowledge acquisition and reasoning process, and an information retrieval process for design-induced error reasoning in real accident reports and the Worldwide Web.

1.7 Limitations of the research

From the research aims above, it is important to note that there are also boundaries to the research:

- This research is not a pure psychological human error study, but a hybrid between cognitive theories and engineering and information technology.
- This research is limited to the study of Design-induced error, not research into all forms of human error.
- This research is not research on how to construct an entire knowledge-based system (KBS), rather to develop an ontology of Design-induced error that may be used in a KBS.
- The research will try to use current Web-based reporting systems, but will not involve changing accident report systems or content of the reports.

1.8 Thesis structure

The fulfilment of the research objectives involves the completion of a series of activities, which in turn define the structure of the thesis which is summarised in Figure 1.2.

Chapter 1 introduces the research issues and research aims/objectives with a broad summary

Chapter 2 reviews literature about human error and design issues in modern technologies. This chapter also reviews theories and phenomena relevant to design-induced error with real accident cases.

Chapter 3 presents research approaches and methodologies by which the research could be conducted.

Chapter 4 develops a meta-theory of design-induced error by adapting ontological assumptions and a contextual paradigm (local rationalities between designer and operator). This work is achieved by investigating underlying structure of theories, and

examining current concepts of design-induced error.

Chapter 5 examines accident reports, which were taken from the Australian aviation accident report system, with the meta-theory, and shows analysis results for the accident cases.

Chapter 6 briefly reviews knowledge acquisition, knowledge modelling methodologies and discusses values of ontology development.

Chapter 7 presents how a theory-based ontology of design-induced error has been developed with a methodology. It includes an overview of the developed ontology of design-induced error.

Chapter 8 discusses, the investigation of the developed methods (a meta-theory, ontology of design-induced error) in this thesis in the light of knowledge sharing (e.g. reasoning support issue, knowledge acquisition issue, and information retrieval issue).

Chapter 9 finally summarises achievements of the research, recommendations for designers and related authorities, and proposed future works are presented.

In order to take both theoretical and practical approaches in this thesis, it was necessary to review the literature on human error and design issues which is reported in Chapter 3 as well as the knowledge sharing issues reported in Chapter 6. From these background studies a theoretical framework and knowledge-based ontology was developed and is reported in Chapter 4 and Chapter 7. Chapter 5 and Chapter 8 are intertwined for completing examination of the theories and applying the developed framework to real accident cases.

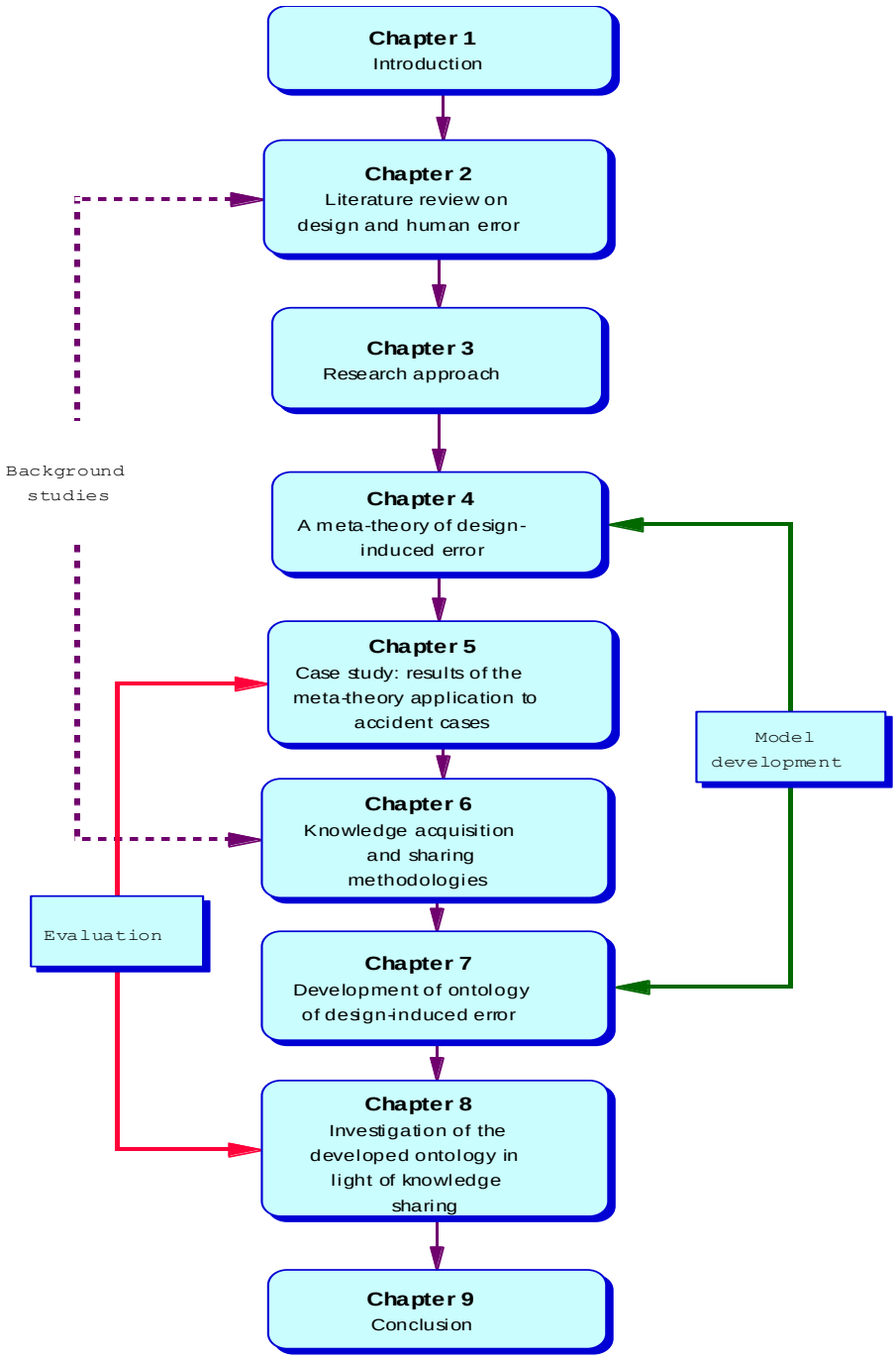


Figure 1.2 Thesis structure

Chapter 2. Literature review

2.1 Introduction

In this chapter concepts of human error and present design-related human error theories are reviewed. This is because the study of human error is the foundation of research into design-induced error. However, it should be stressed that the review does not focus solely on these studies because this is not a study of the psychology of human error, but rather a study of the relationships between design and the consequences of this on the occurrence of types of human error.

2.1.1 Aims and structure of the chapter

The aim of this literature review is to examine theories that present relationships between human error and design, and to identify the characteristics of phenomena that lead to human error. In order to achieve this, it is necessary to examine issues in design of complex and automated systems. This inevitably involves understanding what a human error is, and also the manner in which design affects human cognition and performance. As a result of the need to investigate both of these issues, this chapter contains two main parts. The first introduces a concept of human error, whilst the second examines the design characteristics, especially in modern technologies, related to human error, together with phenomena acknowledged by researchers that are used in this thesis.

Section 2.2 of this chapter will introduce examples to show why we have to focus on human–system interaction failures, and then section 2.3 review the nature and characteristics of human error and its forms. Section 2.4 that follows will discuss theories related to Design-induced error and their relevance to modern complex systems. Section 2.5 reviews theories related to design issues in human error, and examine how the role of design has been changed in the theories. The last section 2.6 will summarise the literature review and present limitations of the current research on finding design issues in human error.

2.1.2 Conduct of the literature review

The basis of this review is literature found from searching databases that were believed to contain abstracts from scientific papers on human error and design issues. This search was conducted using both the web-search engines (such as Ingenta Connect, Science Direct, and BIDS) through Athens connection and an electronic journal service in the Library of the University of Bath. This search concentrated on papers published between the years 1980 and 2005, because many studies on human error have taken place since 1980, and made use of the search terms "human error", "design", and "design-induced error", together with appropriate synonyms of these. Important papers published earlier than 1980 were also reviewed. These searches were conducted both at the beginning and at the conclusion of this research project, to allow the identification and inclusion of relevant research findings that had arisen during the execution of this research project. Accident reports were also collected and analysed. The basic sources of information of the topic of the thesis were found in published literature. Related literature provided cases of accident/incident that contained human error and design issues. The most important sources for collecting accident cases that related to the topic of the thesis were official aviation accident reporting systems (e.g. NTSB, AAIB, ATSB) as well as safety information networks (e.g. Aviation Safety Network) and journals.

This study was conducted by the author to find relevant examples to verify the symptoms of Design-induced error identified from the literature review. Cases were again found through querying (e.g. name of accidents) web-based search engines (e.g. Google.com) or searching in accident databases (e.g. AAIB, NTSB, ATSB). Well-known aviation accident databases such as Aviation Safety Network (http://aviation-safety.net/reports/) were also reviewed.

Given that the aim of this literature review was to find and collect related theories that show human error influenced by design, it was necessary to identify criteria by which to gather related theories. The design concepts of complex and automated systems constructed by using modern technologies are a main focus of design that affects human operators. The complexity and automation in a system should be criteria for identifying design-induced error in human–system interactions. Therefore, the characteristics of modern systems were reviewed in light of human error.

The aim of theories is to explain attitudes towards designed systems held by operators. If it is assumed that the concept of design-induced error is employed as a means to

congregate the value of related theories, then it is necessary to identify the type of characteristics that should be examined to determine whether the concept had been applied to human–system interaction failures. This inevitably requires the identification of possible forms of error outcome. In addition, if a phenomenon is derived from a particular theoretical perspective, the concept of design-induced error encompasses an inclusion of this theory. Consequently, it is necessary to gain an understanding of the theoretical perspective that informs the error.

2.2 Human–system interaction failure

We can find a number of human–system interaction failures in real accident cases. For example, Wiegmann and Shappell (2003) argued that 70~80% of aviation accidents are attributed to human error. Johnson and Holloway (2004) examined Canadian TSB aviation reports between 1996 and 2002 and identified human error as the most common causal factor nearly 56%~75%.. This means that in many cases human operators have failed to interact with systems properly. What are "human–system interaction failures[2]"? In order to understand the risks of automation and complexity in modern design, we must understand the relationship between human operators and automated systems. Sometimes the designer tends to assume that automated systems function independently from the human operator. However, research has shown that humans and machines are not independent. They should work together to achieve the desired purposes of a system [Sarter and Woods, 1995]. The most highly automated systems still require human operators to monitor system activities and intervene in the case of abnormalities and emergencies [Bainbridge, 1983].

Human error research has been developed to tackle the issues of human–system interaction failures. The approach of this research focuses on the role of humans in relation to systems. In other words, most human error research starts from the point of view of the roles of humans in complex and automated systems. This research has provided new insights to understand human–system interaction failures in modern complex and automated systems. For example, the research showed that the human operator often fails to monitor a system when he/she is in a supervisory role [Bainbridge, 1983].

[2] Human−system interaction failures refer to human error. It is preferred in this thesis to use the term "human−system interaction failures" because it is a more value-indifferent term than "human error".

2.2.1 Questions for examples of human–system interaction failures: Origins and motivation for the research

However, this perspective sometimes fails to show clearly and characterise the roles of design in these failures. There still remains a question. What are the exact roles of design in human–system interaction failures? In order to investigate this question and to illustrate the need for a collective view for human–system interaction failures, the following examples of accidents were first considered.

Case 1. Tupolev-154 mid-air collision at Ueberlingen, German/ Switzerland (2002)

On the night of 1 July 2002, there was a collision between a Boeing 757 and a Tupolev-154 above Lake Constance, Ueberlingenm Germany, at 35,000 feet, resulting in 71 fatalities. The Tupolev-154 (registered to Bashkirian Airlines) was en route from Munich to Barcelona at Flight Level (FL) 360, on a heading of 274 degrees. The Boeing 757 (registered to DHL) departed from Bergamo (Italy) to Brussels at FL 260, on a heading of 004 degrees. Both aircraft were equipped with the Traffic Collision and Avoidance System (TCAS). Their trajectories put them on a converging course at a 90° angle in airspace (Figure 2.1).

At that time of the accident, the Zurich Area Control Centre (ACC) was in charge of controlling the airspace. With communication the crew of the Boeing 757, the Swiss controller issued clearances of the B757 climbing FL 360 at time 21.26.36. When the pilot of the T-154 called in the Swiss controller at time 21.30.11, there was a warning from the TCAS systems in both aircrafts. Following this, the controller instructed the T-154 to descend from FL 360 to FL 350 to avoid collision with the B757. However, the pilot of T-154 got an instruction from the TCAS to climb. The crew of B757 also was instructed to descend from the TCAS respectively. After receiving contradictory instructions, the T-154 pilot decided to follow the instruction of the controller and began a descent to FL 350, resulting collision with the B757, which had followed its own TCAS advisory to descend. The pilot might not have believed a direction of the traffic collision avoidance system, but rather followed the instructions of the controller [Nunes and Laursen, 2004].

***Question**: Why the pilot did not follow the instruction of the traffic collision avoidance system?*

Case 2. The rail collision accident at Ladbroke Grove in London (1999)

On 5 October 1999, a three-car train passed a red signal as it was leaving Paddington Station, London, and continued for some 700 metres into the path of a high-speed train with which it then collided. As a result of the collision and subsequent fire, 31 people died and 227 were taken to hospital. A large number of people (296) were treated for minor injuries on site. This accident, as with all major accidents, was the result of a confluence of a series of factors, one of which was the driver's actions. In this case, the driver inadvertently drove through a signal, signal SN109, which had been showing a stop aspect.

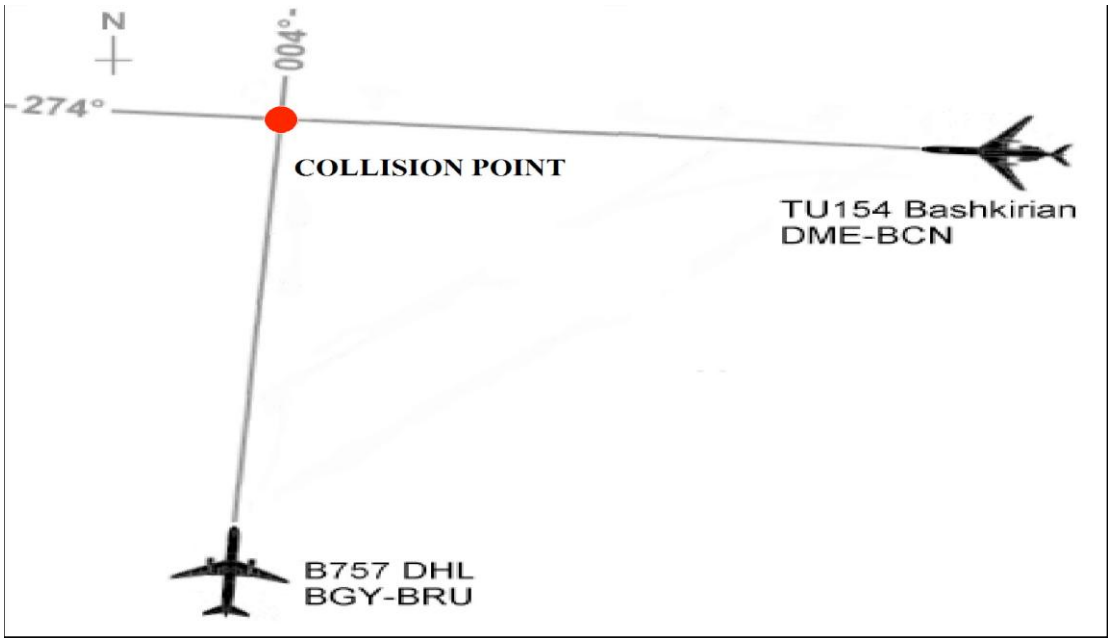


Figure 2.1 Trajectories of B757 and T-154 (from Nunes and Laursen, 2004) [3]

The train, at the time of accident, had an Automatic Warning System (AWS) which consisted of trackside permanent magnets, electro-inductors and inductor suppressors

[3] http://www.humanfactors.uiuc.edu/Reports&PapersPDFs/humfac04/nuneslaur.pdf, 2004

that interface with trainborne AWS equipment. This equipment provides train drivers with an aural and visual indicator of whether an approaching signal shows a clear aspect, a green light, or not. If the signal does not show a clear aspect, it can show a caution aspect, which could be a yellow or a double yellow light, or a stop aspect, which is a red light. The two caution aspects show that although the next track block is clear, subsequent blocks are occupied and therefore the driver should be prepared to stop at the next or next but one signal. If the train travels through a signal showing a stop or caution aspect and the AWS warning is not acknowledged, the brakes on the train are automatically applied.

Prior to the collision, the driver of the three-car train had travelled through three signals: SN43 which had displayed a green light, SN63 which had displayed double yellow lights, and signal SN87, which had displayed a single yellow light. On the approach to signal SN109, the three-car train had been coasting. However, on the approach to signal SN109, the driver increased power, at a point where the signal was not visible, but where other signals on the gantry supporting signal SN109 were. Shortly after accelerating the AWS horn operated to warn the driver that the signal was not showing a clear aspect. Signal SN109 was showing a stop aspect. However, instead of stopping the train, the driver cancelled the AWS warning and began to accelerate at a distance of 107 metres from where the collision occurred.

***Question**: Why did the train driver pass the signal at red?*

Case 3. Chernobyl nuclear accident, USSR (1986)

On 25 April 1986, prior to a routine shut-down, the reactor operator at Chernobyl-4 began preparing for a test to determine how long turbines would spin and supply power following a loss of main electrical power supply. Similar tests had already been carried out at Chernobyl and other plants, despite the fact that these reactors were known to be very unstable at low power settings.

A series of operator actions, including the disabling of automatic shutdown mechanisms, preceded the attempted test early on 26 April. As the flow of coolant water diminished, power output increased. When the operator moved to shut down the reactor due to its unstable condition arising from previous errors, a peculiarity of the design caused a dramatic power surge.

The fuel elements ruptured and the resultant explosive force of steam lifted off the cover plate of the reactor, releasing fission products to the atmosphere. A second explosion threw out fragments of burning fuel and graphite from the core and allowed

air to rush in, causing the graphite moderator to burst into flames.

***Question**: Why did the operator perform a dangerous test against safety rules?*

Case 4. Three Mile Island nuclear power plant reactor overheat, USA (1979)

The accident began about 04:00 on 28 March 1979, when the plant experienced a failure in the secondary, non-nuclear section of the plant. The main feedwater pumps stopped running, caused by either a mechanical or electrical failure, which prevented the steam generators from removing heat (Figure 2.2). First the turbine and then the reactor automatically shut down. Immediately, the pressure in the primary system (the nuclear portion of the plant) began to increase. In order to prevent that pressure from becoming excessive, the pilot-operated relief valve (a valve located at the top of the pressurizer) opened. The valve should have closed when the pressure decreased by a certain amount, but it did not.

Operators in the plant did not recognise the real state of the system. The operator misinterpreted a signal showing the position of the relief valve. Signals available to the operator failed to show that the valve was still open. As a result, cooling water poured out of the stuck-open valve and caused the core of the reactor to overheat.

***Question**: Why did the operators not recognise the state of the system?*

In all these cases, it is difficult to identify any specific failure in the design. For example, the AWS in the Ladbroke Grove accident functioned in the manner it should have, and should have drawn the driver's attention to the signal aspect presented. However, whilst the design of the AWS did not lead directly to engineering failure, the design of the system has helped induce the human operator to develop a specific behaviour.

Use of the system in the above cases appeared to induce a form of automatic or phenomenal behaviour of the operator in the system, which could produce errors that would be undetectable to the operator. These cases depict a need for investigation of the role that design plays in inducing user error, and which can allow designers to gain new insight into how particular designs may function. The origin and motivation of this research is how we can properly and effectively answer the questions above.

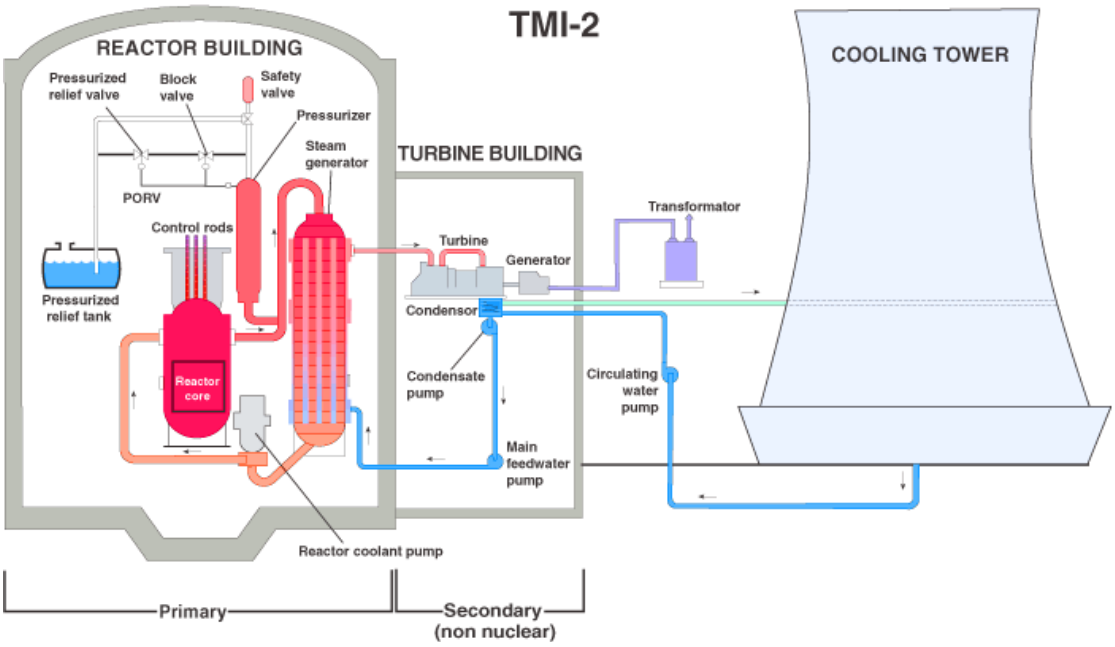


Figure 2.2 NRC: Fact Sheet on the Accident at Three Mile Island[4]

2.3 What is Human Error?

It was not until the early 1960s that the notion of "human error" gained acceptance as a cause of incidents and accidents by many researchers [Reason, 1990]. The field of human error research has expanded to encompass errors that arise in everyday experience, such as errors of language use, to errors made in the operation of complex systems, such as nuclear power plants. Major incidents and accidents such as those at Three Mile Island (1979) and Chernobyl (1986) have emphasised the need for research into human error in many safety critical domains. Driven by these surprising system failures, researchers from different disciplinary backgrounds have begun to re-examine how these systems failed and how people in their various roles contributed to the operation of the system. The research has revealed that there are many problems between human operators and systems. The reliability of a system greatly relies on how the interaction between operators and systems can be achieved. Therefore, human error has gained attention as a main objective of designing reliable systems.

[4] http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html (6 of 6) [3/2/2004 4:25:40 PM])

2.3.1 Level of human performance

Why do humans make errors and what causes the error? To solve the problem, researchers have attempted to identify the physical and psychological limitations in human performance which underlie human error. Those working in the domain of human–machine interaction have paid attention to the limitations and biases in human cognition that affect the processes underlying attention, perception, memory, and logical reasoning [Reason, 1990]. For example, research shows that humans' short term memory can be suffer from difficulty remembering more than seven chunks at once [Miller, 1956].

Reason [1990] suggested that inaccuracies arise in operator models of current and future system states from a number of cognitive processes – i.e. "*frequency gambling*" (i.e. humans are apt to interpret a situation with respect to how many times it has previously happened) and "*similarity matching*" (i.e. humans tend to understand a problem and find a solution based on how much the problem is similar to previous problems). This unique human cognitive process is very effective for humans to do a task and to solve a problem, but sometimes leads to error when combined with a poorly designed artefact (i.e. not considering the unique human cognitive performance) or unusual environments.

The level of our performance changes depending on our experience with the environment, or the artefact. The time taken to act in response to a stimulus will be determined by the level of performance enacted, which is determined by previous experience.

Fiture 2.3 shows a widely accepted model of human performance proposed by Rasmussen - the skill-rule-knowledge-based human performance model [Rasmussen, 1983]. His classification scheme is based on the stepladder model of human performance. In the stepladder model, performance is statically represented by a sequence of states of knowledge, connected together by information processes that involve signals, signs and symbols respectively. He defined the three information factors as follows. Signals represent time–space variables from a dynamical spatial configuration in the environment, signs are related to certain features in the environment and the connected conditions for action, and symbols are abstract constructs related to and defined by a formal structure of relations and processes, including language itself and mathematical equations (p261).

Behaviour is divided into three levels: skill-based, rule-based, and knowledge-based, as shown in the simplified diagram in Figure 2.3.

Skill-based behaviour: is an automated process, requiring little or no conscious control, activated by signals. It generally occurs only for highly practised activities conducted in familiar situations where sensorimotor skills can be utilised (e.g. playing piano by a pianist or driving a car).

Rule-based behaviour: is a routine process, and consists of signs (the execution of stored rules or procedures) that have preconditions that match the current state of the system and its environment (e.g. seeing traffic signs).

Knowledge-based behaviour: is a slow and laborious process, activated by symbols with which human problem solving mechanisms work to define objectives, identify problems, and utilize reasoning (e.g. finding a street with a map). It relies on symbols.

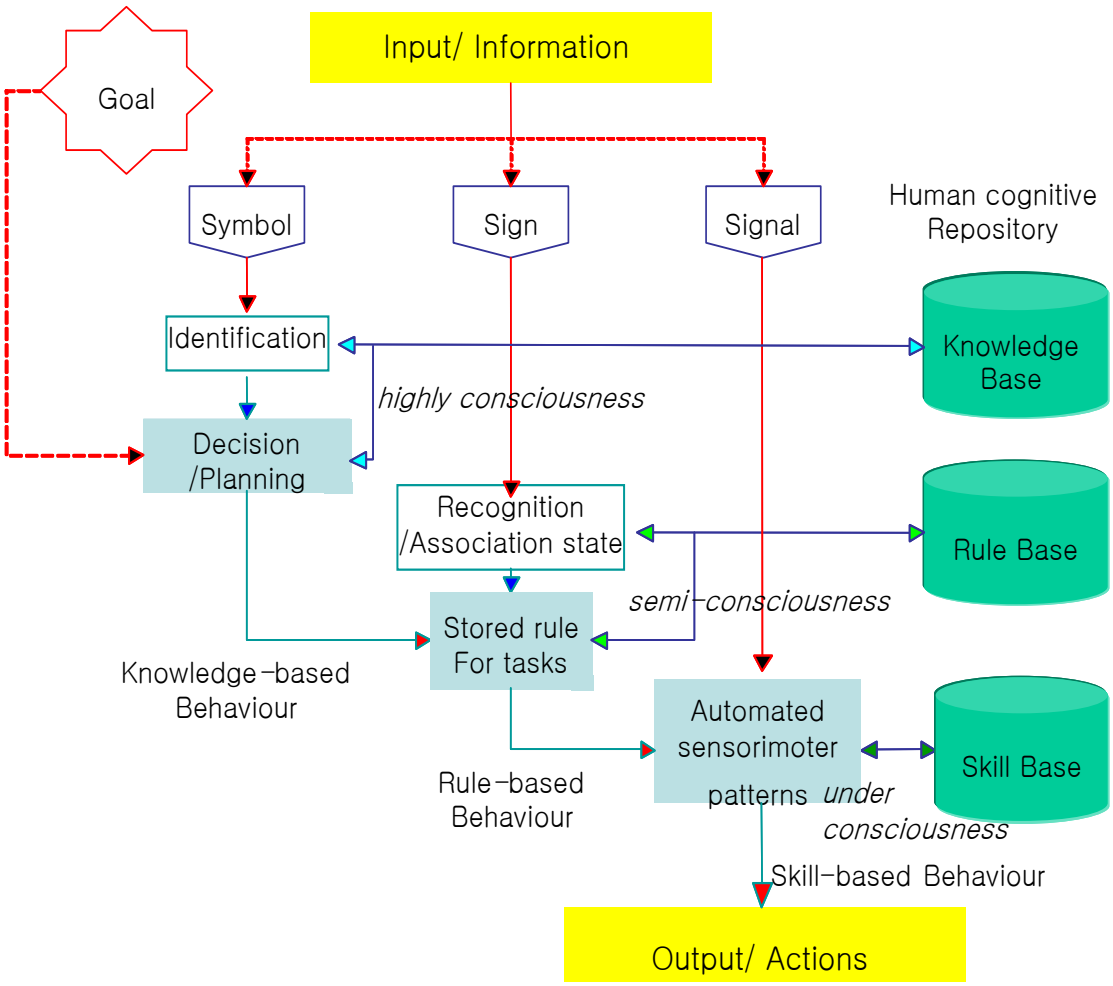


Figure 2.3. Levels of human behaviour (modified from Rasmussen, 1983)

However, it is not clear what are the boundaries between the three types of behaviour, and real performance involves a more complex interaction than just between the three levels. Performance can be optimised by the use of shortcuts, which are learned through experience. However the model is still useful in the identification and organisation of different categories of human behaviour.

Therefore, it is important for designers to know at which performance level operators undertake a task (Table 2.1). Sometimes a task may involve all three levels, for instance, a pilot is in that situation during landing (handling the controls is skill-based behaviour, however, following the air-traffic controller's signal may be rule-based, and checking environmental circumstances may be knowledge-based behaviour).

Table 2.1. Examples of design concerns according to performance levels

PERFORM -ANCE LEVEL	EXAMPLE	DESIGN QUESTION	DESIGN RULES
Knowledge -based	Finding a location in a map	Where is our destination? Is this logical process?	How to provide reasonable ways, methodologies?
Rule-based	Following a traffic sign	Is this rule distinguished clearly?	How to avoid ambiguity among signs?
Skill-based	Driving a car	Is this equipment convenient for a driver to handle?	Does it change or interrupt unconscious actions?

2.3.2 Model of human error

Mach [1905] noted the inseparable nature of knowledge and error: "Knowledge and error flow from the same mental sources, only success can tell one from the other" (p.84). It means that the fact that people's actions that lead to error are not the result of carelessness, but may result from careful reasoning about the system, can lead to conclusions that the designer did not anticipate. However, until the 1980s, it was assumed that normative processes of judgment and inference would ideally follow Bayesian rules. Error was presumed to arise from the use of processes that acted in opposition to normative processes. However research into human cognition has proved that this assertion was wrong and that both correct and erroneous performance arise from the same processes (e.g. Reason, 1990; Hollnagel, 1998). This provides insights for modelling and analysing human error.

Reason [1990] developed a model of human error called "the Generic Error Modelling System(GEMS)", based on Rasmussen's classification of human performance levels. According to Reason's model, human errors can be divided into three types:

1) **Errors at the skill-based level:** which occur during performance of tasks that are not consciously attended to as a result of inattention or over attention (i.e. slips/ lapses).

2) **Errors at the rule-based level:** which arise from the misapplication of a good rule, or the use of a poor rule when the individual has to consciously choose between alternative courses of action (i.e. rule-based mistake).

3) **Errors at the knowledge-based level:** which arise from the selective processing of information about a task, an inability to attend to all the relevant information, or an undue weighting being given to information that comes to mind readily during the individual's attempts to define a new procedure on the basis of knowledge about the system they are using.

2.3.3 Distributed cognition

After researching complex systems, and studies on the manner in which information is transferred between personnel interacting with the system, Hutchins [1995b] defined a theory of *distributed cognition* which described how operators use artefacts in a socio-technical system for remembering and understanding situations and performing procedures.. This theory emphasises an effective collaborative work between operators and artefacts. In a complex system operators are continuously interacting with artefacts and other colleagues to complete tasks set. For example, on a ship a crewman has to work with other crewmembers and artefacts to complete navigation tasks successfully [Hutchins, 1995a]. The theory of distributed cognition could be used to define a framework for the analysis of interaction between operators and artefacts in complex systems. Other models of errors such as Reason's GEMS focussed on errors made by the individual and could not describe or explain the form and origin of errors in collaborative tasks.

Hollan et al. [2000] identified three factors that underlie the manner in which operators effectively use a complex system. First, cognition within a complex system is socially distributed, with representations of the system distributed amongst the operators of the system. A distributed cognition analysis would focus on examining how personnel and artefacts in a system exploit other crewmembers and artefacts to manipulate, represent, and store information. Therefore, research on distributed cognition places emphasis on the manner in which activities are conducted within particular organizational contexts rather than attempting to identify a series of laws that can be used to describe the behaviour of individuals in any setting [Hollnagel, 2001].

Second, cognition is embodied, emerging from the interaction of the mind of the

operator and other components of the system. In other words, the processing conducted within the complex system is not merely in the form of representations in the operators' minds that respond to specific stimuli in the environment [Zhang, 1992]. Rather, the artefacts themselves, and the manner in which they are used support specific practices, and specific processes. For example, work practices associated with specific artefacts may allow the operator to transform a mathematical task into one of visual-spatial judgment [Hutchins, 2000]. In doing this, the operator may reduce the chances of committing an error as they reduce the demand placed upon working memory, under conditions of potentially high mental workload.

Third, culture in the organisation determines the operation of the cognitive system. Within this system, information is propagated with the intention of affecting the representations held by specific operators, using particular modes of communication. Therefore, the study of cognition was not separable from the study of culture. In this case culture was taken to mean the history of social practices in the workplace. The role of culture is to provide partially completed solutions to the problems that are frequently encountered in the workplace. Culture itself was shaped by the activities conducted in particular historical contexts. These principles have been applied to suggest guidelines for the development of robust complex systems.

Hutchins [2000] suggested that there were a number of features that could be incorporated into a system of distributed cognition that would increase the robustness of the system. Principally, these recommendations focussed on the manner in which information was distributed amongst the users of the system and the redundancy inherent in the number of representations acquired by users.

A system may embody consequential communication, in which a system automatically provides physical cues that informs users of its operation [Hutchins, 2000]. For example, in the case of the trim-wheel on the airliner flight deck and the cue this provided, which was removed when the traditional mechanical controls were replaced by electronic ones, the mechanical systems on a flight deck may provide the pilot with a means of assessing whether a particular action has been conducted by another member of the flight crew or not.

Patterns of information flow that create multiple representations of the same state of affairs and the redundant processing of similar information enhance the robustness of the system. These patterns of information flow also support error detection as error detection depends upon the comparison of representations of the same thing developed from different sources or via different processes.

It may be possible to impose patterns of information flow that help to form shared

expectations about task performance by encouraging social distribution of task relevant information. Consequently, the absence of an action in a particular procedure can become meaningful to another operator in the system, indicating a failure in the procedures employed. Such awareness required both operators to know what is expected and to know that the other knows what is to be expected [Hutchins and Klause, 1998].

2.4 Dealing with Errors in Complex Systems and Automation

2.4.1 Complexity and other characteristics in modern systems

Before the recent era of computerised complex information, safety concepts were generally straightforward. The system was not too complicated and complex to enable other people in the system to predict hazards with scientific knowledge. The methods for protecting systems and humans were also well developed technically, with norms, technical guidelines, etc. for directly measuring hazard (e.g. allowance load or strength of a material, temperature of ignition).

In traditional protection systems the primary aim is to increase the safety factors of materials and artefacts according to the hazards of the system. Second, if there is hazard in a system, then safety devices are installed to prevent artefacts from entering unsafe states (e.g. safety valves in boilers) or to mitigate against their consequences. Thirdly, if it is impossible to protect humans who are involved in the system, then the aim is protecting them from hazards by prohibiting them from approaching hazardous components (e.g. installing safety guards) or by providing them with personal protection equipment (e.g. safety helmet, mask). For designers it was easier to design a system in terms of safety and error than it is at present. They could mostly succeed in their goal of system safety by simply following and adapting safety rules.

However, the rapid development of new technologies has caused additional problems. The designer encounters new challenges in current complex and socio-technical system. From the study of the accident at the Three Mile Island nuclear power plant in 1974, Perrow [1984] identify two risk-increasing characteristics in modern complex systems: interactive complexity and tight coupling.

In his explanation, interactive complexity refers to the presence of two or more discrete failures can interact in unexpected ways in a system. The unexpected sequences of events are either not visible or not immediately comprehensible for some critical period

of time for operators. The more tightly coupled a system is, the more highly interdependent and affected each other the status or operations of sub-components of the system is. Small failure of one part, therefore, can cause disastrous failures of the whole system. As a conclusion Perrow argued that due to these two intrinsic characteristics accidents are inevitable or normal in some technological systems [1984].

His argument that accidents are inevitable in these systems and therefore systems in which accidents would have disastrous results should not be built, however, is criticised because of its overly pessimistic view undermining engineering development of complex systems [Marais et al., 2004]. He seems to see systems from the too much organisational point of view not from the engineering design point of view.

Although some refutation against his conclusions, Perrow made an important contribution in understanding characteristics of current complex systems.

Contemporary technologies use automation and automation has three main characteristics: compacting, complicating, and computerisation (Figure 2.4).

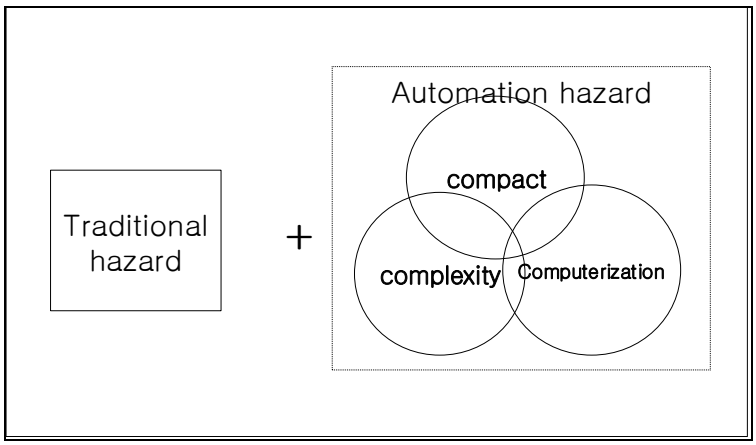


Figure 2.4. Characteristics model of automation with hazard

Compacting means that equipment has tended to be smaller in size, especially in control interfaces with which operators/users control the system. This has produced benefits for human users such as more comfort, and greater ease of handling. However from the cognitive perspective, it has also increased ambiguity and can lead to errors on the part of users by increasing misunderstanding about the system [Reason, 1990]. For example, for seat reservations on UK trains, the old system used reservation cards on the head of the seat that were placed in manually by train staff. In new trains, the seat reservation is written in words on a electronic display over the seat. It is very attractive and can be controlled automatically without manual intervention, but it is less easy to recognise for users.

Complexity is another characteristic of modern technologies. Modern technical systems feature large scale processes and combine them together in systems that require the definition and application of complex organisational and technological inter-relationships to function effectively [Roberts, 1988]. If there is a small error or failure it may cause the failure of whole systems. This is especially true in dynamic systems such as (nuclear) power plants, railway and subway systems, air traffic control, chemical processes, and even in intensive medical facilities.

Computerisation is an intrinsic component of contemporary technology. Computerisation can be defined as the execution by machine, usually a computer, of a function previously carried out by a human [Parasuraman and Riley, 1997]. Development of automation has arisen with microelectronics and computer technologies that are very fast and open a wide range of possibilities. However limitations inherent in the human information processing system means that operators have great difficulty in monitoring changes to the system and updating their mental models of it. There are therefore mismatches and gaps between humans and systems in both space and time. Increased use of automation to reduce the influence of human weakness does not work. Rather it creates new human errors and amplifies existing ones [Lützhöft and Dekker, 2002]. In other word, the key to success of automation systems lies in how they support co-operation with their human operators. For designers, those changes have posed new difficulties in solving problems related to safety and system reliability (Table 2.2).

There are many other factors that mitigate against system failures and human error. Organisational, legal, political and social aspects are also important to achieve the goal of safety. This paper, however, will discuss matters only from the standpoint of human error with design, because human error is one of critical deficiencies in present technologies. It cannot be achieved by technologies alone. We have to know about the user's perspective to understand human error and system failure. Therefore it is proposed to explain several phenomena in a complex system in the light of how the perception of operators deviates from the intention of designers about an artefact.

CHARACTERISTICS	MEANING	EXPLANATION
Complexity	Intangible	Combined process tends to reject showing what is going on a system.
Automated computerisation	Fast	It is faster than human cognition.
Compactness	Unrealistic	Not matched with human tactical perception (e.g. digital screen).

Table 2.2. Characteristics of modern systems

2.4.2 Temporal decision making conditions in complex systems

Increasing use of computer technology has transformed the operator's role in socio-technical systems [Bainbridge, 1983]. One of the most distinguishable points of change is in "temporal decision-making", that it is the decision making process about the progress of an operation, and when intervention in the process should arise [De Keyser, 1990].

In order to design systems that can be effectively used by operators, it is necessary to know how operators decide when to intervene in the operation of the system and the manner in which they use their mental models of the system to estimate both their location in a process, and the duration of the process itself. In addition, there is a need to know how operators use cues from the environment to support their decision-making under time pressure.

Systems and artefacts have evolved into complicated and tightly-coupled forms [Perrow, 1984], and as a result, the speed of systems has increased, leading to quicker completion of actions and faster responses to requests. Operators in the complex system are experiencing conditions that they have not previously met. Problems in temporal decision-making that are encountered in complex systems arise from increases in: (1) time pressure, (2) the number of system functions, and (3) the invisibility of system processes [De Keyser, 1990].

This means that there is a mismatch in the time required for human operators to develop mental models of the system and the pace at which the state of the system can change. The problem space for using the complex system has increased, which means that operators have problems in developing an appropriate mental model of the current state of the system. Their mental models are affected by high frequency of immediate feedback about decisions taken to meet system demands [Reason, 1990].

As noted above, Rasmussen [1983] suggested that there were three levels of performance underlying human decision-making, which were: (1) a knowledge-based level, (2) a rule-based level and (3) a skill-based level. It is clear that the speed of skill-based performance level is fastest, followed by rule-based and knowledge-based performance lastly. In complex systems, human operators may need a knowledge-based performance when they choose to intervene in the system due to complexity of the

system. The system, however, does not allow operators such a time, rather it demands prompt responses, i.e. skill-based performance from operators. People in complex systems have to make decisions under conditions of high time-pressure.

Figure 2.5 shows how a process of operators' performance is changed in temporal decision environments. They have little chances to use a time-consuming knowledge-based process such as identification, decision and planning, but to have to jump into sensorimotors in their skill-based repository.

The operator bases his or her temporal strategies on the checking of specific cues. The operator will focus upon the critical phases of the system's development, where there is a need to intervene in system operation. As the technological development has relocated his or her traditional area of actions, from the process to the whole system, the non-visibility of the team actions increase the complexity of his or her task.

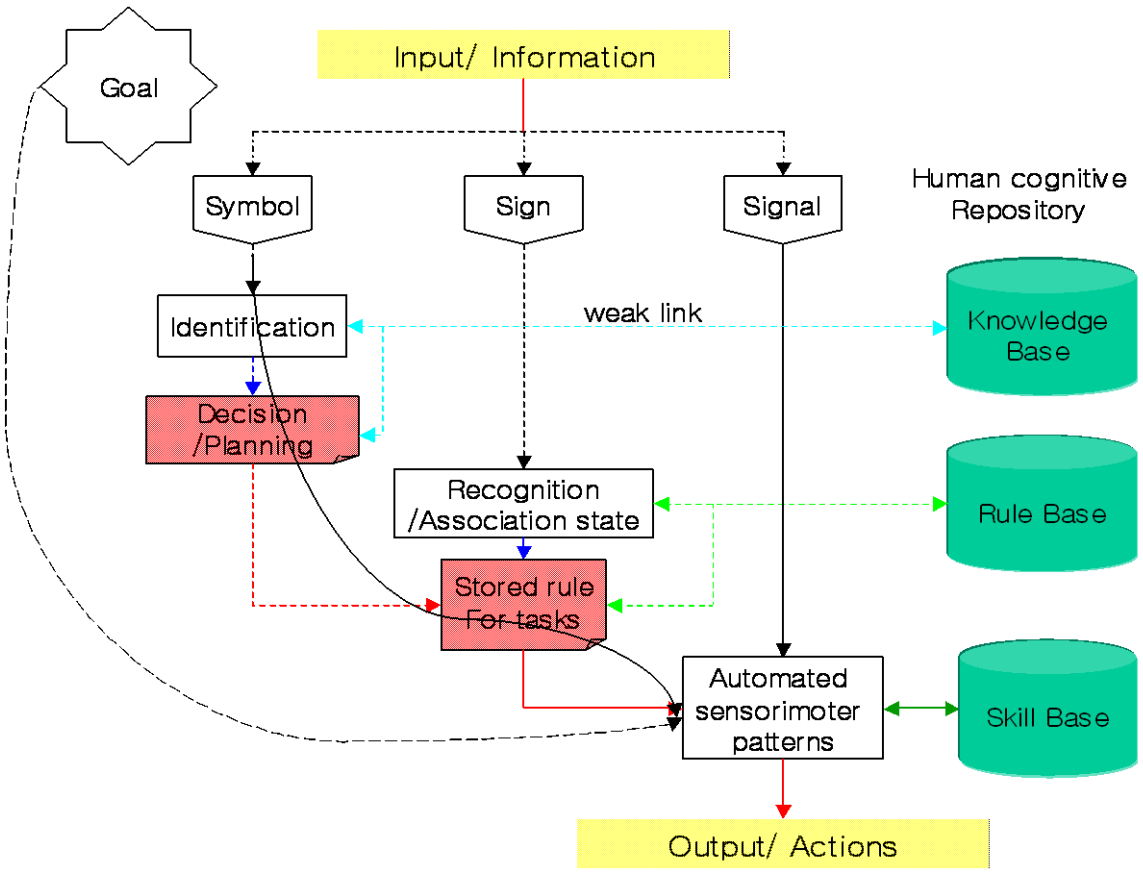


Figure 2.5. A model of the manner in which operators make a temporal decision (modified from Figure 2.3)

Research on distributed cognition has shown that the operation of a socio-technical system relies upon the coordination of the activity of a team of people [Hutchins, 1995]. Now operators might just be presented with a single computer terminal that reports on the state of the system, but might not provide cues as to the actions of others, whereas in older control rooms the layout of the room would make the actions of operators visible to others, such as in the use of mimic boards in power stations.

Temporal decision-making in complex systems has changed the manner in which operators communicate with co-operators as well as artefacts and systems. It has been suggested that, under time pressure or when facing ambiguous system displays, operators use sensemaking to develop their mental models of the system [Busby and Hibberd, 2004]. Their performance levels are also affected with regard to changes of communication and decision-making patterns from considerable reasoning into such as dynamic reasoning, negotiation with systems and instinct. Therefore, the interaction problems between operators and artefacts in complex systems should be considered as design requirements.

2.4.3 Ironies of automation

(USA blackout, 2003) On August 14, 2003, large portions of the Midwest and Northeast United States and Ontario, Canada, experienced an electric power blackout. The outage affected an area with more than 50 million people who were left in the dark for as long as 36 hours. The initial events that led to the cascading blackout occurred in Ohio. Three high-voltage transmission lines operated by an electric company (FirstEnergy Corp) short-circuited when they came into contact with trees that were too close to the lines. The control room operators were unaware of the fault because control room alarm system wasn't working properly, and also unaware that transmission lines had gone down. Therefore they took no action, such as shedding load, which could at that time have kept the problem from becoming too large to control. And FirstEnergy operators, being unaware of the growing problems, did not inform neighbouring utilities and reliability co-ordinators who could have helped address the problem. The loss of three lines resulted in the overloading of nearby lines. But there were also problems at the Midwest Independent System Operator (MISO) the entity that co-ordinates power transmission in the region that includes FirstEnergy. Apparently MISO's system analysis tools were not performing effectively on the afternoon of August 14th, which prevented MISO from becoming aware of FirstEnegy's problems earlier and taking action. They were using out-dated information to support real-time monitoring, which hindered them in detecting further problems in the FirstEnegy system, and that MISO lacked an effective means to identify the location and significance of transmission line breaker operations reported by its monitoring systems. Having that information would have enabled MISO operators to become aware of important line outages much earlier. [US-Canada Power System Outage Task Force, 2004]

As we look at this accident in light of human−system interaction, the operators in the control rooms could not clearly figure out the state of the systems and failed to cope with the abnormal situation. Consequently whole electric systems were shut down although there were several chances to minimise the incident. Automation can hide the internal progress of the systems from human operators and hinders the views of operator to see the circumstances. [Modern Power Systems, 2003]

The electricity generating and distribution industry is one of the industries that adapt a number of complex and automated control systems. However, the above accident case shows how its complex and automated designed systems can easily be vulnerable if

human operators fail to intervene effectively in case of abnormal circumstances. This is a case of ironies in modern automated technologies.

Automation is defined as the means by which operations are done automatically at some level [Sheridan, 1987; Parasuraman et al., 2000]. The dynamic and complex nature of systems and the overwhelming amount of data that must be handled by these systems provides automation with a critical role in planning, decision-making and execution. Shapes and forms of systems have been changed with the introduction of automation. Increasing use of automation is represented in changes to the design of control rooms and the introduction of new technologies such as robots and remote sensing equipment.

Designers have tried to construct more reliable systems. According to Bainbridge (1983) designers may regard humans as the most inefficient and unreliable components of the system, therefore their work has been substituted by automated systems. However there still remain problems because it is impossible for designers to design a system that can be run with no intervention from a human operator [Bainbridge, 1983]. It is impossible for the designer to automate all tasks or to identify all potential states that a system might enter, and so there is a need to include a means to mitigate against these problems – a human operator. However, automation leads operators to lack practice in operating the system. In the above case of the USA blackout in 2003, the operator in the control room did not correctly recognise the problem due to their lack of understanding in such an abnormal situation.

Therefore automation can fail in many ways. Bainbridge pointed out three things induced by the introduction of automation without considering humans. First, automation requires that designers produce systems that can cope with component failure rather than rely on operators whose role during operations has been changed by automation. These changes require that the designer anticipate and correctly address all possible failure scenarios. However, systems sometimes fail to produce corresponding response signals to warn operators of problems. For example, the system in the above accident case did not provide relevant warnings or information on the relationship between the problem and causes. Inaccurate automation-aids may cause errors and system failure.

For this reason, design errors can be a major source of operating problems. In the case of the USS Vincennes incident in 1988, when a US warship shot down an Iranian passenger plane, the naval crew misidentified the target in the computerised Aegis display. In July 1988, the USS Vincennes was patrolling the restricted waters of the Persian Gulf with the Aegis missile defence system onboard. The Aegis system

displayed an attack by an incoming Iranian F-14 fighter. On the basis of information displayed on the Aegis user interface, the crew believed that the fighter was rapidly descending to prepare for an attack approach on the ship. The crew of Vincennes fired two missiles in order to defend themselves. However, it was not Iranian F-14, but a civilian aircraft, Iran Air Flight 655. The missiles destroyed the airplane resulting in the loss of 290 lives. [ASN, 1988]

In later analysis, one of the designers of the Aegis display interface reported that the altitude information was difficult to interpret correctly. Aegis is highly automatic. Threats are identified and targets selected and tracked. It is an autonomic system with a sense-model-act architecture. In this instance, the threatening aircraft altitude was not shown on the main display, but required that the operator request it, when it would be shown in a sub-window with other ancillary data. And rather than show a rate of altitude change (as is common in aircraft displays), the altitude of the threat was shown as a numeric display, requiring that the Aegis operator do mental arithmetic to determine altitude increase or decrease – difficult in normal circumstances, although clearly learnable. But under the stress of battle it would be all too simple to make an error in arithmetic, especially while the display is rapidly changing. Thus, it would be simple to believe that the unknown incoming jet really was in an attack flight pattern, and difficult to believe it was not a hostile aircraft [Russel et al., 2003].

Second, automation is included as a means to reduce the degree to which operators intervene in the operation of the system as a means of reducing the number of actions taken by unreliable human operators. This has led to human operators being given a task that they are unsuited to, the monitoring of the system over long periods of time. For example, a DC-10 tried to land at John F. Kennedy Airport, New York, in 1984, touching down about halfway down the runway and about 50 knots over target speed. A faulty auto-throttle was probably responsible. However, the flight crew, who apparently were not monitoring the airspeed, never detected the over-speed condition [Wiener, 1988].

Third, as the designer cannot anticipate all conditions that a system may encounter, or may make errors in the design of the system, automated systems can reach abnormal states that require the intervention of a human operator. As a result, human operators still remain as a component of the system, with the role of diagnosing abnormal system states. These exceptional states, however, correspond to the most challenging and obscure problems. Human operators may be unable to respond to these problems as automation leads to an absence of opportunities to practising problem diagnosis. Furthermore, operators may not be aware of the state of the system, because humans are not suited to maintaining vigilant monitoring of a system over a long period of time.

Psychological studies have shown that humans are most prone to mistakes in these types of tasks, especially when automation has eliminated normal day-to-day interaction with the system. They suffer from detecting abnormal situations due to low vigilant ability and degraded skills. Bainbridge named this problem mentioned above as "the ironies of automation".

2.4.4 Trust in automation

(Northwest Airline air crash, 1987) Northwest Flight 255 departed Saginaw for a flight to Detroit, Phoenix and Santa Ana, arriving at Detroit (DTW) at 19:42. Pushback for departure was accomplished at 20:34 and the crew received taxi instructions for runway 3C. During the taxi out, the captain missed the turnoff at taxiway C and new taxi instructions were given. At 20:42 Flight 255 was told to taxi into position on runway 3C and hold, followed by a takeoff clearance two minutes later. Shortly after rotation the stick shaker (stall warning) activated. The aircraft rolled left and right and the left wing struck a light pole in a car rental lot. Flight 255 continued to roll to the left, continued across the car lot, struck a light pole in a second rental car lot and struck the side wall of the roof in a 90deg left wing down attitude. The plane was still rolling to the left when it impacted the ground on a road outside the airport boundary and continued to slide along the road, striking a railroad embankment, disintegrating and bursting into flames.

PROBABLE CAUSE: "The flight crew's failure to use the taxi checklist to ensure that the flaps and slats were extended for take-off. Contributing the accident was the absence of electrical power to the airplane take-off warning system which thus did not warn the flight crew that the airplane was not configured properly for take-off. The reason for the absence of electrical power could not be determined." [ASN, 1987].

Originally, pilots manually extended the flaps and slats, performed any manoeuvring needed if a stall did occur, and were responsible for the various other tasks needed for take-off. Due to the increase in automation of the cockpit, however, they now depend on automation to perform the pre-flight tasks reliably and without incident. Pilots have now been delegated to the passive role of monitoring the automation and are to interfere in its processes only in emergency situations. The accident was caused partly by the crew's trust and reliance on the aeroplane's automation to configure for take-off and failure to confirm the configuration with the use of the taxi checklist. The accident provides an example of how automation has transformed the role of pilots [Prinzel, 2002].

Bainbridge's [1983] discussion of the concept of ironies of automation suggests that an operator's ability to deal with problems that arise in the operation of a system has been decreased by automation. The role of the operator has now become one of system supervisor. In order to effectively operate the system, the operator has to place

appropriate trust in the automation underlying the system.

Within social psychology there has been recognition of the importance of trust in activity. For example, the performance of an economic system is dependent upon the degree of trust that individuals have in it. If people fail to trust a market system the whole system will be disrupted in a moment, as demonstrated by the 1929 great panic in America. Based on models from social psychology about how people would trust one anther, Muir and Moray [1994] attempted to define a model of trust in automation.

With the development of automation the concept of trust has became important in technological fields as the role of human operators has been restricted to supervision of the system. The interface of the system may make it difficult for the operator to understand the operation of the system as the mechanisms of computerised and tightly coupled systems may be hidden from view. For example, in the Üeberlingen mid-air collision accident (2002), the pilot in one aircraft suffered from a decision making problem as to which instruction he had to follow, between the air traffic controller and the Traffic Collision and Avoidance System (TCAS) fitted in the aircraft.

In automated systems, decisions about managing the system depend on the operator's perception and understanding of data from the system shown on control room visual displays. These views represent virtual images because the images of the state of systems on the screen represent a filtered view of the system gathered from sensors within the system. Therefore, it is important for systems to give operators information that can be trusted. It was suggested by Muir that trust is the product of three factors; *predictability*, *dependability* and *faith.*

The theory of trust in automation attempts to describe the manner in which an operator develops faith in a system and their attitudes towards the system. If an operator uses a tool to help her/him accomplish a task, s/he is seen as trusting the tool to some degree. It is related to the dependability of the system as well as the predictability of the system. From this perspective, trust in systems depends on the frequency of success the operator has had in using the system during recent operations. Although operators may place trust in one part of a system's automation, this might not extend to all the automation within a system. In other words, trust can be partitioned, the operators may trust the different sub-systems to different degrees, depending on how these sub-systems behave.

Designers would hope that operators would trust a system because trust in automation can increase the productivity of the system. For example, operators in a system who trust the system may be able to make decisions about system use more quickly than those who do not trust the system. To do this it is necessary to increase the perceived

reliability of that automation by design. However, there are a number of factors that would hinder and reduce the degree to which operators trust the system's automation, such as unsuitable monitor systems, false alarms, etc.

As we saw in the discussion of the concept of the irony of automation, systems need human intervention even in systems with high levels of automation. For good intervention of human operators, the operator has to be aware of the unpredictability in system operation that arises from unpredictable environmental conditions, and the inherent unpredictability in the system. The following case has been discussed many times among researchers as to why the automation system affected the crew in the ship, who neglected to check correctly the state of an automation system until the ship was close to a critical point.

> In the Royal Majesty incident, on 9 June 1995, the cruise ship Royal Majesty which left St George's, Bermuda, at about midday bound for Boston had sophisticated systems at that time. The ship was equipped with an Integrated Bridge System (IBS) consisting of an autopilot obtaining position (NACOS 25) data from GPS and a navigation unit (Loran-C). While cruising the crews did not in doubt about position of the ship. However, the GPS switched to dead-reckoning mode because it was no longer receiving satellite signals shortly after departure. The GPS antenna was later found to have separated from its cable. The autopilot tracked the GPS "data" until the ship grounded on the Nantucket shoals. There was substantial cost for the incident.
>
> [Lützhöoft and Dekker, 2002; Husemann, 2003; NTSB, 1995]

Trust has negative effects as well as positive, and these have been termed *over-trust* and *under-trust*. Under-trust leads to disuse (unuse), whilst over-trust leads to misuse by operators. Under-trust is represented by failure of trust in automation. When automation provides false diagnoses or chooses a tactic to accomplish tasks with which the operators disagree, trust declines. Faults in systems also increase mistrust in the automation. For example, on 7 February 1993, at London Gatwick Airport, a Boeing 747-243 suffered problems while landing, the pilot had to make three attempts at landing before a safe landing was made. At the second approach, the pilots ignored the information being presented to them on the flight deck, which was correct, because in their first landing trial they used the Automatic Flight Control System (AFCS) but it failed, so they, therefore, thought the automatic system had deficiencies [AAIB, 1994]. However, the most common issue is over-trust.

Automation-Induced Complacency is another term for inappropriate trust in automation. According to the Aviation Safety Reporting System (ASRS) coding manual [EATMP,

2003], automation-induced complacency is defined as “self-satisfaction, which may result in non-vigilance based on an unjustified assumption of satisfactory system state”. When working in highly reliable automated environments in which the operator serves as a supervisory controller, monitoring system states, operators tend to fail to find the occasional automation failure [Sarter et al., 1997].

2.4.5 Automation surprises

(Strasbourg air accident, 1992) On January 20, 1992, an Airbus A320 (Air Inter flew) crashed into a mountain on a night during approaching to Strasbourg, France, killing 87 of the 93 people on board. Following an uneventful flight from Lyons the crew prepared for a descent and approach to Strasbourg. At first the crew asked for an ILS approach to runway 26 followed by a visual circuit to land on runway 05. This was not possible because of departing traffic from runway 26. The Strasbourg controllers then gave flight 148 radar guidance to ANDLO at 11DME from the Strasbourg VORTAC[5]. Altitude over ANDLO was 5000 feet. After ANDLO the VOR/DME[6] approach profile calls for a 5.5% slope (3.3deg angle of descent) to the Strasbourg VORTAC. While trying to program the angle of descent, "-3.3", into the Flight Control Unit (FCU) the crew did not notice that it was in HDG/V/S (heading/vertical speed) mode. In vertical speed mode "-3.3" means a descent rate of 3300 feet/min. In TRK/FPA (track/flight path angle) mode this would have meant a (correct) -3.3deg descent angle. A -3.3deg descent angle corresponds with an 800 feet/min rate of descent. The Vosges mountains near Strasbourg were in clouds above 2000 feet, with tops of the layer reaching about 6400 feet when flight 148 started descending from ANDLO. At about 3nm from ANDLO the aircraft struck trees and impacted a 2710 feet high ridge at the 2620 feet level near Mt. Saint-Odile. Because the aircraft was not GPWS[7]-equipped, the crew were not warned. [ASN, 1992]

Thanks to modern digital technologies, the design of control equipment has changed and now typically incorporates compact, computerised graphical displays. This has certainly been the case in the aerospace industry. The term "glass cockpit[8]" has been introduced in recent years to reflect these changes [Sweet, 1995]. This term refers to the current generation of airliner flight decks that incorporate these new technologies. These systems were introduced to increase the precision and efficiency of airliner operations.

[5] VORTAC: Very High Frequency Omni-Directional Radio Range Tactical Air Navigation Aid

[6] VOR/DME: VHF Omni-Directional Radio-Range/Distance-Measuring Equipment

[7] GPWS: Ground Proximity Warning System

[8] The term "glass cockpit" is colloquial but has been used in aviation research papers.

Such cockpits replace a myriad of gauges, switches, and indicators with several computerized display systems. By using computers to manage the on-board systems, pilots are able to call up what they want to see when they want to see it. This has allowed modern aircraft to require only two crewmembers instead of the three needed by their predecessors. However, at the same time, serious problems have arisen related to breakdowns in the interaction between human operators and automated systems. Great technological advances also place much greater burdens on the designers and users of these glass cockpits [Bartolone and Trujillo, 2002].

Through the graphical displays in a glass cockpit crucial information is conveyed to pilots. If the information is misread, misinterpreted, or misunderstood, the results could be catastrophic. Knowing this, the developers of such electronic systems must be sensitive to how human beings interpret, and misinterpret, data displayed on a screen. It has been reported that pilots using FMS (Flight Management Systems) have experienced occasionally being unable to maintain awareness of which mode the aircraft was in [Sarter and Woods, 1995; Hutchins, 1995b].

The term "automation surprise" was introduced by Sarter et al. [1997]. A failure to keep the operators informed can lead to what have been euphemistically described by them as automation surprises, whereby the system does something which the operators do not understand in the current context. Sarter used the term for a glass cockpit situation instead of usual term "mode error". Mode error traditionally refers to the problem that the user has in keeping track of the mode a device is in. The automation surprise happens in cases where a system can enter a state that was not explicitly expressed to users and not expected by them.[Sarter et al., 1997]. The Bangalore air crash, below, illustrates the problem of automation surprise.

> The aircraft departed Bombay at 11:58 hours local time, on 14 February 1990, for a flight to Bangalore-Hindustan airport, Bangalore. While on final approach after being cleared for a visual approach to Runway 09, the aircraft descended below the normal approach profile. The steep descent continued until the aircraft touched down on a golf course (2300 feet short of the runway and 200 feet right of the extended centreline), skidded for several hundred feet, impacted an embankment, and caught fire. Failure of the pilots to realize the seriousness of a high rate of descent at a low altitude, and increase engine power accordingly with the aircraft's Auto-Flight system operating in Idle/Open Descent mode was discovered. During the approach for landing, the pilots accidentally selected a control mode called "OPEN DESCENT", and were then unable in the time available to work out what they had done wrong. In this particular mode, the aircraft cuts back engine

> power and thereafter maintains its speed by progressively losing height. As a result, the rate of descent is immediately too great for safe landing, and, by the same token, the aircraft is guaranteed to undershoot the runway. The "OPEN DESCENT" mode therefore makes it impossible to maintain a meaningful approach to landing, or to override the lack of power, locking the aircraft into certain disaster unless and until the mode is cancelled. The pilots only discovered their error 10 seconds before impact, leaving them too little time for the idling engines to re-spool up to thrust. [ASN, 1990]

On 24 April 1994 a China Airlines Airbus 300-600 crashed while on approach to Nagoya Airport, Japan. During the approach the co-pilot inadvertently engaged the aircraft's "go-around mode," which caused the automated systems to attempt to fly away from the ground using the aircraft pitch trim system, while the pilots attempted to continue the landing approach via input to the elevator. The pilots were unable to determine that the pitch trim input of the autopilot system was causing difficulties controlling the aircraft. Additionally, the design of the A300 autopilot (at that time) did not allow the pilots to override the autopilot by use of opposing control stick pressure. Thus, the pilots and automated systems continued to struggle for control, with the aircraft eventually pitching up to near vertical, stalling, and crashing on the approach end of the runway – killing 264 passengers and crew. In this accident, the pilot experienced unexpected performance of the autopilot system in the flight [ASN, 1994].

2.5 Design Issues with Human Error

Design and human error are related. Many useful theoretical concepts have been developed to show how inappropriate design can lead to human error. This section introduces several issues related to how design can promote human error.

2.5.1 Problems in the use of Information transfer systems

Designers' ideas are produced in the form of artefacts. The ideas and knowledge of the designer are embodied in the form and function of the artefact. There is knowledge that the designers intend to express. However, the designer's knowledge may not be apparent to the user of the artefact as a result of limitations in the expression space of the artefacts. Users or operators understand the ideas embodied by the designer in the artefact through contact with and use of the artefact. However, this use and the operator's perceptions of the artefact are mediated by their experience and common knowledge. Therefore, there is the possibility that operators will misinterpret what the designer wanted to deliver to users.

Psychological research reveals that human beings tend to worry about disconnections between information and knowledge [Festinger, 1975]. For example, when an operator encounters unknown or unfamiliar artefacts during the conduct of a task, he or she tends to carry on with the task rather than try to infer information from the artefact of system using his or her experience and cognitive knowledge.

When we see information flow from designers to users (Figure 2.6), the ideas of designers about artefacts are transferred into users through the artefacts. However, the meaning of ideas that designers really want to deliver cannot be correctly interpreted by users unless the users' knowledge and experience match with the ideas of the designers because there are no direct contacts between designers and users. If the knowledge and information inferred from the artefact by operators is different from that the designers expect users to infer, we can say that there is a deficiency in the information transfer system.

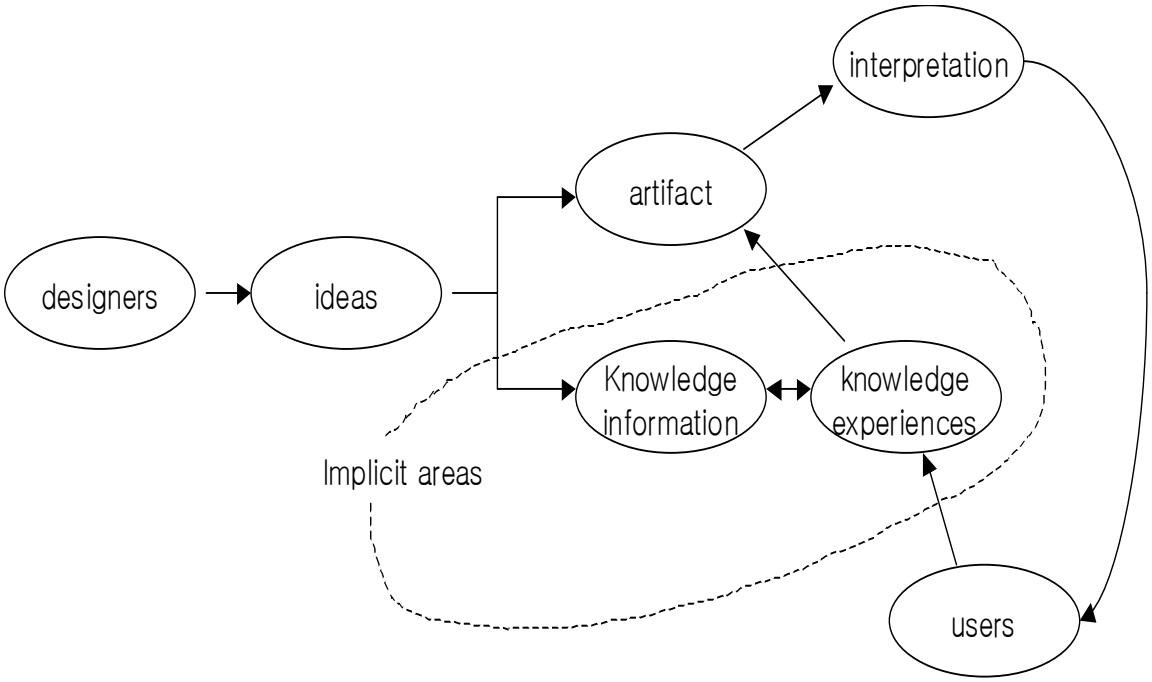


Figure 2.6. A model of the manner in which information is transferred between designers and users

2.5.2 Design affordance

(Scottsbluff train collision, 2003) On February 13, 2003, about 12:25 p.m., an eastbound Burlington Northern Santa Fe Railway (BNSF) unit coal train collided with a BNSF yard train on the main track in Scottsbluff, Nebraska. The coal train consisted of 2 locomotives and 124 loaded cars; the yard train consisted of 1 locomotive and 16 freight cars. Both locomotives of the coal train and 28 cars of coal derailed; the locomotive and 3 cars of the yard train derailed. The crew of the coal train consisted of an engineer and a conductor. The engineer received minor injuries, and the conductor sustained fatal injuries. The crew of the yard train consisted of an engineer, a conductor, and a brakeman. The engineer said that he could see the switch banners, but not the switch points. According to the engineer, the switch banners were "all green" as he proceeded eastward. He mistakenly thought that this indicated that the route was lined for a straight movement in the direction of the lead track. Although the display indicated that the yard switches were lined for movement down the lead track, the green switch banner on the inside switch indicated that this switch was lined for a diverging movement onto the main track. Had this switch been lined for movement on the lead track, as the engineer intended, its switch banner would have been yellow [NTSB, 2003]. They just followed the signal according their cultural perception that green sign mean they allow to go.

Conceived by Gibson [1977] the term "affordance" refers to the perceived and actual properties of an artefact, primarily those fundamental properties that determine just how it could possibly be used [Norman, 1998]. For example, a chair affords ("is for") support and, therefore, affords sitting. A chair can also be carried. Every artefact has its own affordance. If designers design an artefact with features against the affordance perception of users, the user perceives the properties of the artefact in different ways. For example, if a knob is installed on a device, a user perceives that the knob has a function of changing the setting of the device by controlling the knob, although the designer designed the knob for a different purpose.

For the designer the concept of affordance is closely related to the functions of artefacts. Designers include a number of features in an artefact that are related to the artefact's function. They expect that these features lead users to understand by implication their function. On the contrary, the meanings (e.g. function) that the designers intend to provide may be not well delivered to operators if the artefact does not have enough affordance. Humans intrinsically perceive the functions of things by identifying the artefact's physical affordance (in shape, size, or sound).

Modern electronic systems, however, have lost many of the characteristics of physical affordance that the previous generation of mechanical systems would have possessed. Especially, in automation systems physical affordances are melted down into monitoring screen represented as digital numbers or graphics. In these systems affordances are represented in the form of graphics on visual display units. The design of human–computer interfaces does not have to include any correspondence between the content of the display and the physical system. The affordance of artefacts provides indications as to the functions of the artefact. In modern automation technology, therefore, it is necessary to expand on the concept of affordance and employ it in the analysis of the content of the computerised visual display units and associated aural annunciator that form part of many contemporary systems [Norman, 1993].

In the case of the Ladbroke Grove train collision (1999), the reason the driver of the accident train passed a signal at red while cancelling the warning alarm may be related to the concept of affordance. It is conceivable that the driver was not aware that an error had been made. The driver was inexperienced, and so may not have noticed that the train was proceeding onto the wrong section of railway track. Although the driver would be expected to periodically assess the progress in an activity, even following the use of an automated set of skills, this requires that there are cues which indicate that an action has deviated from that planned [HSE, 2000]. Although there had been previous

incidents when signal SN109 had been passed at danger, these had been by experienced drivers who had recognised the error when their trains had been directed onto the wrong section of railway track.

It was suggested in the report of this incident [HSE, 2000] that the cancellation of the AWS could have been an automatic response. The AWS warning does not distinguish between caution and stop aspects. On the approach to a major station, such as Paddington, the volume of traffic means that many of the signals that drivers encounter would show caution aspects. As a consequence, drivers cancel AWS warnings on a regular basis, which could lead to a potential automation of their response. In this case, the driver may simply have mistakenly believed that the AWS warning at signal SN109 indicated that it was possible to proceed. He was not alone in experiencing problems whilst driving in the Paddington area. Signal SN109 recorded one of the highest levels of Signal Passed at Danger (SPAD) incidents on the UK Railtrack network [HSE, 2000].

In this case, designers made functions for the warning signals and expected operators to distinguish the signals between red and yellow even if the sounds were the same. However, the meaning of information is different for the actual operators in the trains.

Affordance provides strong clues as to the operation of things. For example, slots are for inserting things into. Balls are for throwing or bouncing. When affordances are taken advantage of, the user knows what to do just by looking; no picture, label or instruction is required. Such properties make things easy for the user of an artefact. We hold a pencil in such a way that it fits comfortably in the hand, ignoring the myriad less appropriate ways that it might be grasped. The pencil affords being held in this way as a result of its length, width, weight, and texture, which correspond to the size, configuration, and musculature of our hand. Further, we can see most of these properties and relationships; we can often tell how to interact with an object or an environmental feature simply by looking at it, with little or no thought involved.

Affordances in the physical world are an intuitive notion, easily described and understood through example. Like many such concepts, however, it is difficult to define in precise analytical terms. Imagine yourself in the act of sitting down in a chair. There are at least four separate affordance-related concepts involved. First are the affordances proper: the seat of the chair is horizontal, flat, extended, rigid, and approximately knee-high off the ground, all relative to your own proportions and position. Second is perception of these properties, the surfaces, distances, areas, textures, relationships between parts, and so forth. Third is the mental interpretation derived from the perceptions. Fourth and finally is the act of sitting itself. An examination of these positions will give a better understanding of the subtleties

involved.

If affordance fails it causes human error. For example, researchers found that in the 1940s, pilots often retracted the landing gear instead of the landing flaps after landing. This was because the designers had put two identical toggle switches side-by-side, one for the landing gear, the other for the flaps [Chapanis, 1999]. Pilots might fail to identify the gear/switches because of the similarities in their positions and in shapes.[Norman, 1992].

There are three issues in affordance for design. Good affordances allow users to use the artefact very easily without laborious cognitive efforts because they are well connected with humans' expectations in constraints and mapping (e.g. sign "R" means right position). Wrong affordance induces wrong action for users. For example, a door has a handle suggesting it can be pulled but it does not provide the function correctly. Missing an affordance is another problem of affordance. If any artefact does not provide any affordance about how it works, people will be confused about what to do with the artefact.

Affordance can be regarded as a series of conceptual spaces that underlie a user's reasoning about an artefact and its state. Flach and Dominguez [1995] suggested that there were three conceptual spaces: an affordance space, a control space, and an information space. The affordance space is those functions that can be performed on a particular system through the user interface. The control space is comprised of the set of inputs that the user can make via the system controls. Information space represents the output the system presents to the operator through auditory and visual displays. It is suggested that the control space can constrain operators to safe modes of operation. The control space also may reduce the working memory load of operators attempting to complete specific tasks.

The concept of knowledge in the world suggests that well developed artefacts can provide operators with relevant information that meet the need of the operators to represent and manipulate all the information required to complete a task within working memory [Norman, 1993].

2.5.3 Action cycle and Gulf[9] of execution/evaluation

(American Airlines air accident, 1995) On December 20, 1995, At about 18:34 EST, American Airlines Flight 965 took off from Miami for a flight to Cali. At 21:34, while descending to FL(flight level) 200, the crew contacted Cali Approach. The aircraft was 63nm out of Cali VOR (which is 8nm South of the airport)) at the time. Cali cleared the flight for a direct Cali VOR approach and report at Tulua VOR. Followed one minute later by a clearance for a straight in VOR DME approach to runway 19 (the Rozo 1 arrival). The crew then tried to select the Rozo NDB (Non Directional Beacon) on the Flight Management Computer (FMC). Because their Jeppesen approach plates[10] showed 'R' as the code for Rozo, the crew selected this option. But 'R' in the FMC database meant Romeo. Romeo is a navaid 150nm from Rozo, but has the same frequency. The aircraft had just passed Tulua VOR when it started a turn to the left (towards Romeo). This turn caused some confusion in the cockpit since Rozo 1 was to be a straight in approach. 87 Seconds after commencing the turn, the crew activated Heading Select (HDG SEL), which disengaged LNAV and started a right turn. The left turn brought the B757 over mountainous terrain, so a Ground Proximity Warning System (GPWS) warning sounded. With increased engine power and nose-up the crew tried to climb. The spoilers were still activated however. The stick shaker then activated and the aircraft crashed into a mountain at about 8900 feet (Cali field elevation being 3153 feet) [ASN, 1995].

Hutchins et al. [1985] described a model of an "action cycle" (Figure 2.7) which they believed described the cognitive processes a human employs to attain his or her goals. In their model, there are seven processes in the action cycle, that are divided into two sets, *execution* and *evaluation*. In the execution part there are three stages; the intention to act, the description of an action sequence to attain a goal, and execution of that action sequence. When we set a goal we formulate an intent to act so as to achieve the goal.

The actual sequence of actions that we plan to conduct is followed by physical

[9] The term "gulf "coined by Norman has been used in human computer interaction to describe gap or mismatch between user's goal for action and the means to execute that goal.

[10] Approach Plates is a common term used to describe the printed procedures or charts, more formally Instrument Approach Procedures(IFR), that pilots use to fly approaches during IFR operations. (http://encyclopedia.thefreedictionary.com/Approach+Plates+)

execution of that action sequence. The "evaluation" aspect also has three stages; perceiving the state of the world, interpreting the perception according to our expectations and evaluation of this interpretation in relation to what we expected to happen. As executions are made people try to perceive its sequence and the stage of the world where they act. After that we compare and interpret current states with prior state and interpret according to our expectations. Finally we evaluate the interpretation with what we expected to happen.

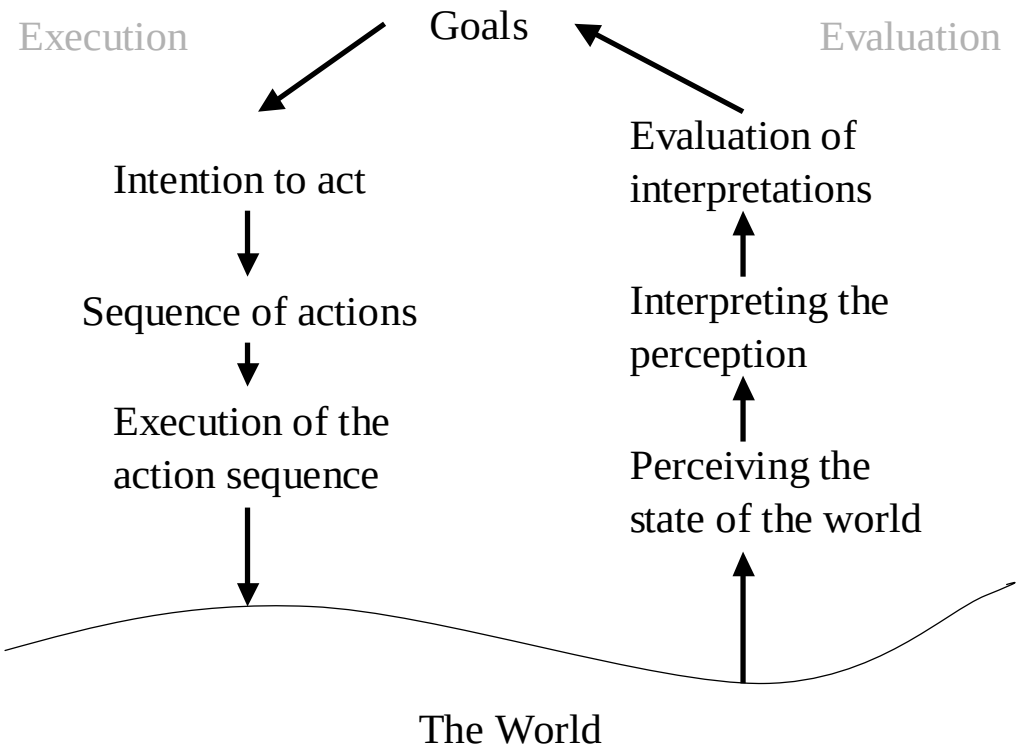


Figure 2.7. Action cycle (from Norman, 1998)

A human may need media to contact the world. It means that most our perception and actions depend on an interface by which the interaction with the system would be mediated. For the action cycle we need intermediate devices to achieve goals. In modern technological systems human actions act on control equipment. In the operation of complex systems, users typically exchange information with the program that controls the physical artefacts within the system through the user interface.

Designers would like operators to carry out tasks by exploiting artefacts in the manner that designers expect. Designers also wish that operators would follow a pre-defined problem solving procedure if they encounter problems with the system. However, operators may not act in the manner that designers expect.

Gulf of execution refers to the difference between intended action and the actions that

the operator believes that the system will allow. For example, in a computer software program an operator wants to interrupt a procedure of the program and change into other procedure, but the program (designers) do not expect that case and expect the operator to wait until the procedure has finished. The designer does not provide the operator with an appropriate menu to cancel the preceding operation and change to the other procedure. This is the case of mismatch between the user's intention and the allowable actions. It is important that a capability of design might exist but that this might not be apparent to the user from the user interface.

The most famous case of gulf of execution was the Therac-25 radiation treatment equipment accident in Texas in 1986. A radiation machine called Therac-25 was developed in order to treat malignant tumours. The equipment was designed to have two modes; "Electron mode" and "X-ray mode". The first mode was low-energy mode and the latter was a high voltage mode with a grid to reduce the radiation density. The mode was changed by an operator simply entering the signs ('x' for X-ray mode or 'e' for electron mode) on the computer screen. In one of the accidents involving the machine, when an operator in charge of the equipment in a hospital clicked a start button to treat a patient, she immediately recognised she had made a mistake. She needed to treat the patient with the electron mode, not the X-ray mode. She pressed the up arrow, selected the "Edit" command, hit 'e' for electron mode, and hit 'enter', signifying she has completed configuring the system and was ready to start treatment. There was an error message. She did not understand the meaning of the message. To solve the problem, she re-entered a "beam ready" command. She tried it again desperately several times. The patient died four months later. The problem was that the change of modes never occurred because of the error function, and additionally the grid was removed from its position. Therefore the patient was exposed to full power of radiation. It turned out that this particular sequence of actions within this timeframe had never occurred in all of the testing and evaluation of the equipment. There were no feedback and execution cues that operators needed [Levenson and Turner, 1993].

If a system does not provide users with a semantic result of an action done to achieve a goal, there is a *gulf of evaluation*. The semantic result means that it should be represented in the form comparable with the goal (e.g. show achievement/target in a graph). The gulf of evaluation refers to the amount of effort that the operator has to invest in deciding what the state of the system is compared with a goal. It also refers to whether the operator can interpret the state of the system from presented information, which might not be the case. For instance, when an operator enters data, but the system does not show the entered data with a goal, but just shows the entered data only in the screen because the designer expects the user to know well the goal. The user has

suffered from not knowing how much he/she has achieved and has to do for the goal. This is mismatch between the system's representation and the user's expectations.

The phenomenon of the gulf of evaluation have been found a number of accident cases, as for example, the case of Methotrexate[11] toxicity of a patient of the UK National Health Service:

> In 2000 a woman died of Methotrexate toxicity. She had been treated for rheumatoid arthritis since 1997. Doctors who treated her prescribed a dose of Methotrexate 17.5 mg once a week. In January 2000, the patient underwent an operation to replace her right knee. As a result the dosage of the drug was altered from 17.5 mg weekly to a daily 2.5 mg dose during her entire stay of eight days. On 6 April 2000, she and her daughter asked a GP (General Practioner) to prescribe Methotrexate in a way that involved taking fewer tablets, as experienced in hospital during the patient's January 2000 admission. The GP agreed and issued a prescription for Methotrexate 10mg tablet, entering the prescription "daily" inadvertently into a computer although the intention had been 10 mg "as directed". Therefore, Methotrexate 10 mg daily was recorded on the General Practice's computer. The community pharmacist dispensed Methotrexate 10 mg once daily. Therefore the patient took one 10 mg tablet daily and total dose of 70 mg a week following the directions printed on the medicine bottle. On 12 April 2000, another GP was on duty signing repeat prescriptions and received a repeat prescription request from the patient. The GP recognized the dose of Methotrexate was incorrect, and interpreted this as a one-off error by the staff producing the prescription. It seemed impossible to the GP that such a dose could have been previously prescribed or dispensed. He therefore crossed out the word "Methotrexate" on the prescription, anticipating that a correct prescription would consequently be presented for signing. The GP did not inspect or change the patient's computer drug record. As a result, an incorrect recoding remained on the computer. … No one had recognised the symptoms of her condition until after she died. [Cambridgeshire

[11] Methotrexate is a folic acid antagonist and is classified as an antimetabolite cytotoxic immunosuppressant agent. It has been used for many years as a therapy for cancers such as leukaemias, lymphomas and solid tumours such as breast and lung cancer. It is also used to treat severe forms of psoriasis, a chronic skin disease, and has been widely used as a disease modifying drug for rheumatoid arthritis. Because of its potential toxicity, however, Methotrexate needs to be carefully monitored particularly for adverse effects on the bone marrow and liver.

Health Authority, 2000]

It appears that the GP who wrongly prescribed the drug had no intention of changing the patient's total weekly dose of 17.5 mg, but to simplify it by reducing the number of tablets to be taken from seven tablets to four once weekly (1 x 10 mg and 3 x 2.5 mg – the patient already had a supply of 2.5 mg tablets). However, it has been identified that the GP made an inputting error into the practice-based computer entering the abbreviation "od" (once daily) instead of "asd" (as directed) into the computer. This error resulted in the prescription being generated from the computer stating "Methotrexate 10mg daily". At the time of this event the practice's computer system did not have any warning message about Methotrexate and its weekly dosage regime. Also the pharmacy computer system did not have any warning message about Methotrexate and its weekly dosage regime.

The suppliers of Methotrexate tablets market 2.5 mg and 10 mg strengths as yellow tablets. The 2.5 mg tablet is scored on one side with "M2.5" and is pale yellow, whilst the 10 mg tablet is scored "M10" and is a deeper yellow colour. The tablets are the same size and shape.

One of the design problems in this case is how to prevent users from entering wrong data inadvertently. Systems were needed to provide users with relevant results of the input data for feedback. If the computer system gave a result of the total amount of dosage of the drug the doctor would have recognised his fault of input data easily. The designer of the computer system omitted evaluating whether the input data is relevant or not. The designers may think that users check input data if they thought the data were important. However, users of the computer tend to believe the computer system, thinking the computer evaluates the data and shows the results when the data are invalid. Such types of different understanding between designers and operators on a system are shown in many accident reports. For example, in the Three Mile Island nuclear power plant accident in 1979, operators failed to recognise that the relief valve was stuck open because the indicator on the control panel misled them. The indicator only showed the commanded state of the valve, however the operator thought the indicator showed the actual state of the valve [Perrow, 1984; Reason, 1990].

We can see other example of gulf of evaluation in the case of East Midlands airport accident in 1989.

> On 8 January 1989, an aeroplane flew into the bank of the M6 motorway while trying to land at East Midlands Airport, UK. The left engine of the aeroplane failed, but the crew shut down the right (functioning) engine by looking at displays (Figure 2.8). They struggled with the problem for many minutes until

> the realised their mistake, by which time it was too late to take corrective action. The crew believed that their objective was achievable by following a particular course of action, but the actions they took closed down the space of future interaction possibilities, and the feedback they received did not alert them to their misunderstanding of the state of the system until it was too late. [AAIB, 1990]

The cockpit system is very complicated (Figure 2.9). At the time of hectic conditions, situations impact on human cognition. The investigation report suggested new designs that consider increased human perception (Figure 2.10). The execution gulf happens when preparing an action, while the evaluation gulf exists when evaluating the action. The causes of these gulfs mainly originate from designers' poor expectations about operators [Norman, 1998].

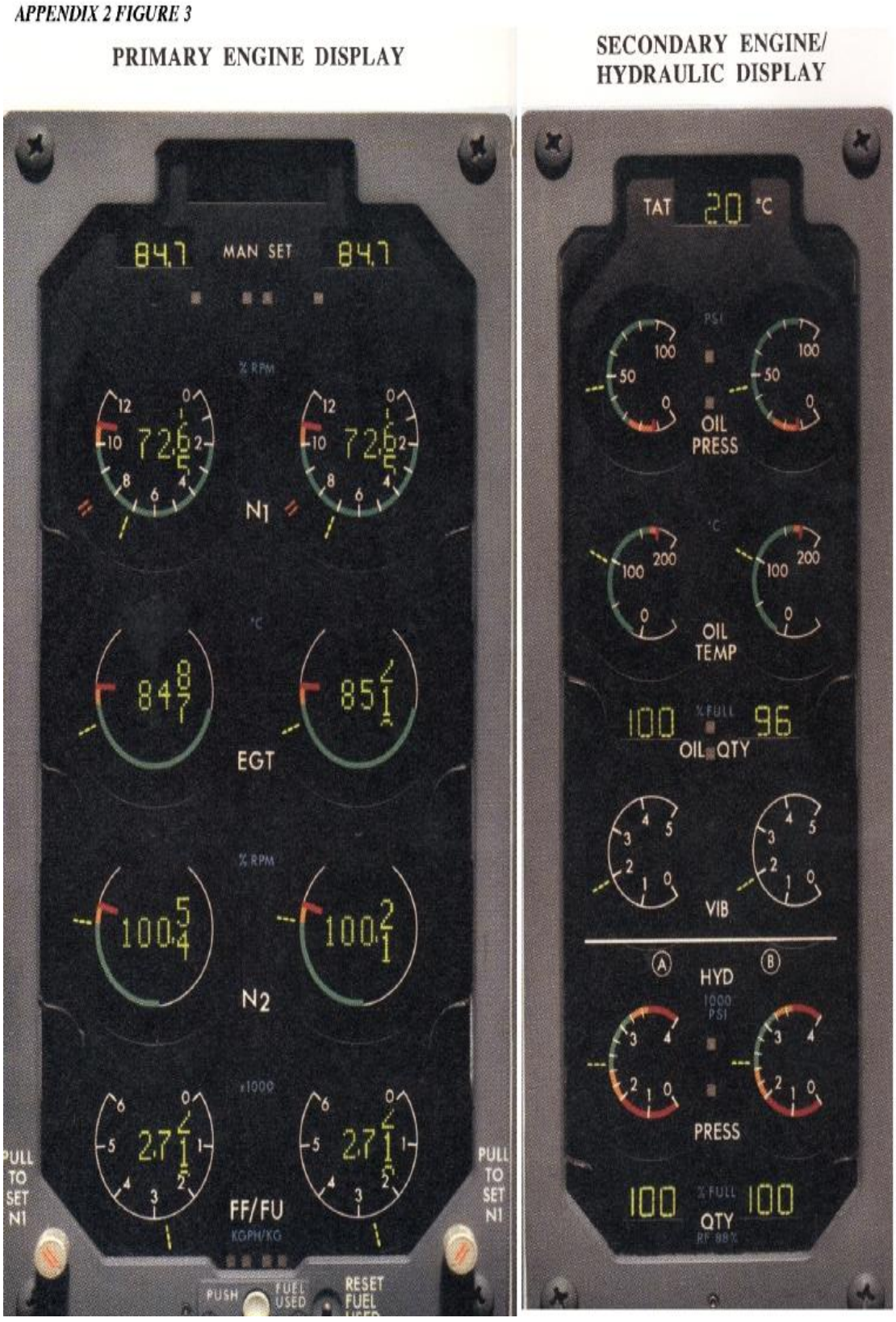


Figure 2.8 Indicators of both engines (AAIB, Aircraft accident report 4/90, 1990)

SHOWING HYBRID ELECTROMECHANICAL POINTER/LED COUNTER INSTRUMENTS USED FOR DISPLAY OF ENGINE PARAMETERS WITH VIBRATION INDICATORS ARROWED

APPENDIX 2 FIGURE 1

Figure 2.9 A view of cockpit control room (AAIB, Aircraft accident report 4/90, 1990)

If the instruments are all to be located on the front panel, two possibilities are apparent. The first is to mount the secondary instruments to one side of the primary instruments as in Figure 2.

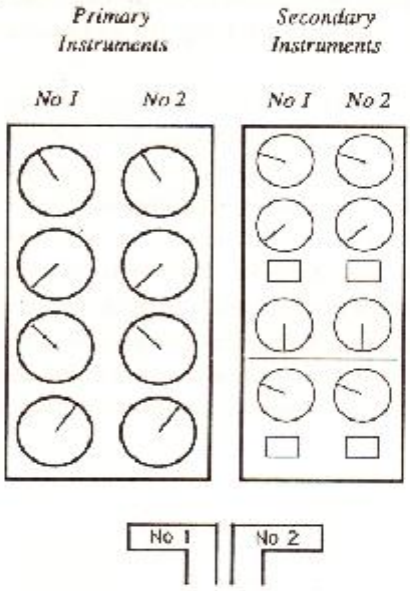


Figure 2

The second is to split the secondary instruments and mount them outboard of their respective primary instruments, as in Figure 3.

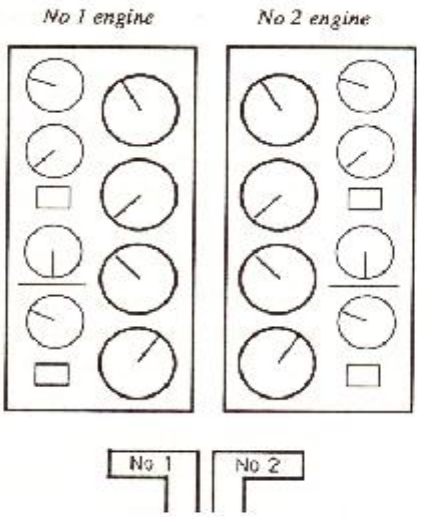


Figure 3

APPENDIX 2.7 A–2

Figure 2.10. Recommendation for human-oriented design (AAIB, Aircraft accident report 4/90, 1990)

2.5.4 Risk homeostasis

(Titanic disaster, 1912) On April 10, 1912, the new Royal Mail Steamer, Titanic, flagship of the White Star Line, cast off from Southampton, England, on her maiden voyage to New York. She carried 2,208 passengers and crew. 4 days after her departure from the port, she was crossing the middle of Atlantic Ocean. At 11:40 p.m. on April 14, one of the lookouts, stationed in the crow's nest, noticed something in the distance. He rang the warning bell three times, signalling the bridge of an object directly ahead, and picked up the bridge-crow's-nest telephone. A terse exchange over the telephone effectively warned the bridge of the impending danger, however, the warning had come to late to avert a collision. She broke in two and then sank into the deep sea with over 1,500 lives lost.

During the entire voyage the weather was clear and the sea was calm with sunshine. On the third day out from port ice warnings were received by the wireless operators on the Titanic, and at least three of these warnings came direct to the commander of the ship on the day of the accident, the first about noon, from the Baltic, of the White Star Line. This message places icebergs within five miles of the track that the Titanic was following, and near the place were the accident occurred. The second message was sent from the California, another ship which was cruising near the Titanic, reporting ice about 19 miles to the northward of the track that the Titanic was following. The third message was reported from the Amerika. The final message was sent by the California reading " We are stopped and surrounded by ice." The reply of the Titanic; "Shut up. I am busy. I am working Cape Race." The Titanic was just following the track where reports by other ships warned there was ice. No general discussion took place among the officers; no conference was called to consider these warnings; no heed was given to them. The speed was not reduced, the lookout was not increased, and the only vigilance displayed by the officer of the watch was by instructions to the lookout to keep a sharp lookout for ice [USA Senate inquiry report].

Why did not the crewmembers in the ship reduce speed and prepare for the danger? Why did they ignore the warning signals reported by preceding ships? Why did they take the risk? *Titanic* was constructed with new technology at that time, the designers adopted everything that supported the functionality including performance, capacity and safety. It was said of the safety of the ship: "In the event of an accident, or at any time when it may be considered advisable, the captain can, by simply moving an electric switch, instantly close the (watertight) doors throughout, practically making the

vessel unsinkable" (The Shipbuilder, 1912). The ship was supposed to stay afloat for days until assistance arrived. Operators including the Captain might be confident about the technology embodied in the ship. This plan only worked, however, if only four compartments were flooded. At the time of the accident, the iceberg breached five compartments.

According to risk homeostasis theory, there is a propensity for human beings to depend on systems and to act more dangerously if they think that this system is more reliable than one that performed the same function that they had used before [Wilde, 1982]. As a result, the introduction of new systems with enhanced safety features may feature the same total risk as preceding systems. For instance, car manufacturers develop and install safety devices (e.g. ABS, air bags, safety belts) designed to protect drivers and reduce risk. However, the driver tends to drive at higher speeds because they believe the systems are safer, negating the reduction in total risk that the safety devices were designed to promote [Wilde, 1998].

The designers of the *Titanic* might have wanted the ship to be the safest as well as the most luxurious one in the world. Therefore, a number of newly emerging technologies such as safety systems which included a double-skin hull (the bottom space divided into 73 watertight compartments), 19 bulkheads and electric doors, 48 lifeboats and advanced water pump technology had been adopted to help to increase the reliability of the ship by reducing risk. However, the system could not help in avoiding the risk of the operator's wrong decision [Kozak, 2003].

The nature of humans is to be risk taking to some degree when they feel the circumstances are safer compared to a previous situation. For example, a jaywalker may pay more attention when crossing a road than a pedestrian who is crossing at a crossing-point designated for them. Safety devices provide better means for increasing safety in many areas. However, these devices do not affect people's desire to take greater risks. Risk homeostasis has also been called risk "compensation theory" by Peltzman [1975].

Peltzman [1975] showed how human beings change one risk to another risk. He explained that the decrease in car-occupant deaths in highway fatality rates was exactly matched by increases in non-occupant deaths. Therefore offset behaviour of drivers had nullified the potentially beneficial effects of the new safety standards. Other studies of traffic-related accidents suggested that the introduction of several automobile safety regulations (e.g. in the 1970s, safety related rules were introduced in the USA such as wearing of seat-belts on highways, etc.) is ineffective in the long run [Geller, 1995; Streff, 1998]. They showed that the total level of injury risk may be unchanged if the

regulation simply reallocates risk from one activity to another, or from automobile users to groups of pedestrians, cyclists and motorcyclists.

People have a level of risk they will accept to accomplish a particular task. If a safety device is included in a system, they will behave in a manner that is consistent with the level of risk they will accept. Consequently, if a car has a safety device such as ABS, this means that the individual moving from a non-ABS equipped car will believe that if they transfer their non-ABS driving behaviour to the ABS-equipped car, the overall risk from driving will decrease. However, as the individual recognises that this is below their accepted level of overall risk for driving, they will modify their driving behaviour to improve the productivity of the task until they reach the same perceived overall risk as would be the case in driving the non-ABS equipped car.

Reason [1997] also suggested that the reduced risk associated with exploiting a specific range of system affordances might lead the user to believe that he or she can exploit a greater range of system affordances. In other words, increased protection is exploited as a means of gaining increased production, or increasing the efficiency with which a task can be conducted. It is argued that efforts to remove causes of human error by incremental improvement of system design is ineffective due to the adaptive risk compensation of operators [Rasmussen, 1999]. For example, in the case of the Chernobyl nuclear accident in 1986, operators in the system did not think it would cause an accident even though they knew they violated safety rules. They tried to continue tests with getting rid of some safety devices. One of the operators said: "We had many experiences of excessive removal of rods, I'd say – and nothing happened…", "No one of us could envisage those actions could cause nuclear accidents. We knew these actions were prohibited, but we never thought …" (quoted in Gorbachev, 2003).

Designers attempt to reduce risk by increasing the reliability of systems with protective equipment such as safety devices. Most work achieved by designers who have tried to reduce risk and increase reliability of systems is also related to productivity and economic reasons. There are several ways to accomplish risk reduction and increasing system productions. These include: accurately computing reliability, increasing use of automation, inclusion of safety devices for operators, adding protection to systems, and including emergency systems. With these safety systems, therefore, appearance (surface) risk seems to be lowered more than in the past for operators, which can lead users to have over-confidence in the use of the system. These factors contribute to the development of new and unexpected risks [Adams, 1995].

Designers have cut down costs of systems by using more accurate computational techniques that lead to reduced safety margins as well as reduced risk of failures of the

systems. In the past the structures of artefacts and systems were bigger and stronger than current artefacts or systems due to larger safety margins provided for system safety. The designers of the system involved in the Chernobyl nuclear accident in 1986, believed that their safety technology had reduced the risk of a nuclear power plant failure. They decided to build the nuclear power plant near to a densely populated location to save electrical loss. The plant was constructed without a cover, believing in the safety systems and abilities of the operators.

Artefacts and systems, however, have become more and more slim and compact in structures and features. Although the system has become more accurate and complex, this change has been accompanied by a reduction in the margin for error.

When hidden risk induced by safety systems is added to the apparent risk, the real risk (actual risk) appears. Hidden risk consists of unexpected risk and new risks induced by design of systems.

Real risk = apparent risk + hidden risk induced by safety systems

Therefore, although reliability of systems is increased, the real risk remains the same. Sometimes significant of the risk may be even higher or bigger than before. In fact, actual risk may not be reduced greatly compared with before. Risk hidden in modern systems is not well detected due to its scale and the tight-coupled mechanisms of system and the inclusion of additional safety devices [Perrow, 1984]. Apparent risk is reduced by a number of safety devices, protection systems and emergency systems.

Human operators, however, tend to assume that apparent risk is the same as the real risk. Thanks to increased reliability and amount of safety systems, operators feel they have a chance to exploit systems to a greater extent, and to increase the performance level of the system. Consequently, they tend to act more dangerously than before, which can lead to their encountering an unexpected risk [Reason, 1997].

Combining human nature on risk taking and over-confidence in systems, users occasionally forget the limitations of the system. That leads to negligence or ignoring of warning information and sometimes they exploit the systems, violating some safety rules. Therefore, the characteristics of risk homeostasis in terms of human interaction with systems can be described as risk taking and risk alteration.

2.5.5 Decision reasoning and plan delegation

In complex systems there is a need to prepare some planned behaviour by operator and maintenance staff in order to maintain the integrity of the system [Rasmussen, 1987]. The roles of that behaviour are called 'plan delegation' [Busby and Hughes, 2003]. Designers expect that operators and maintenance personnel do their work according to the process that the designer planned even though it might not be explicitly expressed in manuals or instructions. However, the operator and maintenance staff believe that the designer has prepared a device that will cope with abnormal circumstances. Absences or misunderstandings about plan delegation, therefore, imperil the system. Plan delegation is of extreme importance at the time when changes are made to the system states (e.g. start-up, shut-down, dismantling and reassembling).

2.6 Summary of the literature review

The literature review that has been conducted has examined two main issues. Firstly, there has been an examination of the research on the manner in which error occurs. Secondly, there has been an examination of the phenomena that are related to design and human error. The purpose of this section is to summarise what we have achieved in research on human–system interaction failures, and what is still needed to develop methods for use from the results of the research. Table 2.3 summarises the literature review.

Table 2.3 Summary of literature review

LITERATURE REVIEW STEPS	THEORETICAL BACKGROUD	FINDING (UNDERSTANDING ON BEHAVIOUR ON DESIGNED ARTIFACT)
Study for human error	– General Human Error Modelling Systems (Section 2.3.2) – Distributed cognition theory (Section 2.3.3)	– Three modes of human error in different human performance levels (skill-based, rule-based, knowledge based performances) – Cognition in a complex system is socially distributed, embedded with representations in artificial systems, and they are connected each others culturally
Identifying issues in complex systems and automation issues	– Characteristics of complex systems and automation (Section 2.4.1) – Temporal decision making condition theory (Section 2.4.2)	– The complex and automated modern systems create new types of situations for operators – what human operators encounter during operation in a complex system are time pressure, the number of system functions and the invisibility of a system processes
Finding theories related to design issues and human error	– Ironies of automation theory (Section 2.4.3) – Trust in automation theory (Section 2.4.4) – Automation surprise (glass cockpit problems) theory (Section 2.4.5) – Design affordance theory (Section 2.5.2) – Gulf of execution and evaluation theory (Section 2.5.3) – Risk homeostasis theory (Section 2.5.4) – Plan delegation theory (Section 2.5.5)	– Although the increase of automation of systems, operators suffer from monitoring or degraded abilities to deal operational condition with such as emergency – Operators tend to rely on automated systems not to intervene actively – Operators often fail to identify representations of systems correctly – Representations in systems not well communicate with operators – Reliability of systems increase a possibility of trust in the systems – Psychologically Uncomfortable design lead for operators to making errors – Operators expect usability of artefact designed on the artefact itself

2.6.1 Issues addressed by previous research

Thanks to psychological studies on human error, that have examined why failures in interactions with artefacts arise, we can expand our knowledge of how to produce more reliable designs. Reason [1990] illustrated how our cognitive structures can lead to error. His error types, such as slip and mistake in terms of levels of performance, provide good explanations of the manner in which people perform tasks and the role that experience and physical and psychological constraints have on the occurrence of error. We also have some understanding of the manner in which human operators exploit and communicate within a system. Following is a summary of the literature review:

- Human error is still one of the main concerns of developing a credible system.
- Indirect human–system failures have increased, as systems have become more automated and complex.
- Theories have developed to explain such failures.
- There are several theories that concern design issues in human–system interaction failures.

2.6.2 Limitations of previous research

This chapter examined theories related to human error and design problems. The theories showed that even though modern design has developed more credible systems there has been still difficulty for human operators to make errors while interacting with artefacts/systems in modern complex, automated, and computerised systems. Each theory explains well specific phenomena of human error in a system, and how designs of the system lead the operator in the system to making errors.

Although each theory uses a different metaphor to explain phenomena, there is a common underlying meaning: raising design issues that lead a human operator to make an error. The understanding of the operator in a system is different from the original purpose of the system.

However, it is not only one theory that presents design issues in human error. Several theories were found that that explain the issues, and none has tried to provide a collective view of the theories (e.g. in terms of the role of design in human error). As a

result, theories are isolated from each other and appear to explain issues in different ways. There is no integrating approach to combine theories with a specific point of view, even those theories addressing similar issues. That may confuse readers researching design issues in human error.

The need to conduct this research was prompted by the lack of an integrating model that can provide a collective view of related theories. For example, if a designer want to analyse his/her system with regard to human error and safety, it is necessary to review related theories. It takes time and effort. Sometimes the designer may miss an important theory that should be considered in the design. If he/she has a method to see a collective view on theories, it will be easier for him/her to recognise design issues than before.

Accident analysts may also have a problem with interpreting human−system interaction failures. If they want to try to investigate design issues in the case, they need an interpretational tool for the case. None of an integrated model for theories may hinder them to pick up the issue effectively.

Chapter 3. Research approach

The literature review in Chapter 2 examined general human error models and characteristics of modern design concepts, and highlighted difficulties of human operators who have to carry out tasks in temporal decision making conditions that are created by employing the modern design concepts, such as automation, complexity and abstract features, that are prevalent in today's systems. The previous chapter finally identified seven theories that explain phenomena in which the design of systems exploits cognition and performances of human operators in contact with modern artefacts. These theories however have not been classified or integrated for readers to understand more systematically the influences of design on human operators. They stand alone without connection to each other. This has prompted a need to develop a model that contains the theories within the same paradigm (or category) by identifying characteristics in the theories relating to each other in conjunction with design and human error, which help to identify design issues easily in human error cases.

This study was carried out to develop methods by which hidden influences on human operators can be better understood. Therefore a concept of design-induced error which represents unexpected influences of design adverse to human operators or users in a system was introduced by integrating current theories which represent these phenomena. This study also explored terms and phrases described in accident report documents in order to examine the possibility of capturing the concept of design-induced error in human error cases.

This chapter describes an overview of the research approach and methodologies that were used in this research. In order to achieve this it is first necessary to identify the research objectives that need to be addressed and the issues that must be considered to meet them. This research had two main aims: developing a theoretical ontology (i.e. meta-theory of design-induced error); and developing a practical ontology (i.e. a knowledge-based ontology used in knowledge management systems) of design-induced error. For the former aim ontological methodology was adopted in order to synthesise related theories, which are relevant to a concept of design-induced error, from an extensive literature review and investigation of accident cases. For the latter aim an ontology editor (i.e. PC PACK) for knowledge acquisition and ontology construction tasks was adopted.

The reason ontology was chosen as a fundamental methodology of this research is presented in the first section (Section 3.1). Designing the research approach and

description of research processes follow.

3.1 Meeting the research objectives: Why ontology was used in the research

In the introduction (chapter 1), it was stated that the main objective of this research was to develop an appropriate model for the explanation of interaction failure between humans and systems in terms of the role of design (i.e. a concept of design-induced error). The fulfilment of this research objective requires gaining an understanding of design issues that would affect human cognition and performances. This, in turn, requires the fulfilment of two additional research objectives.

Firstly, there is a need to identify relevant theories which address design issues that lead to human error in order to develop an appropriate theoretical model. The relevant theories are comprised in the model developed because the model is a kind of meta-theory.

Secondly, there is a need to choose a methodology by which we can capture the contextual factors of design-induced error that exist in accident reports. The methodology should be applicable for knowledge acquisition and annotation (mark-up) and ontology building from accident documents because an accident report system was chosen for applying the meta-theory of design-induced error. With the developed knowledge-based ontology of design-induced error, a designer can be provided with the means to understand and reason on design issues related to human−system interaction failures.

In order to achieve the objectives, this research adopted *ontological methodology* as a conceptual methodology because ontology is considered as the theory of items and ontological methodology is a process to create ontology of a specific domain [Poli, 2002].

According to realist philosophers of science, the complex nature of phenomena can be regarded as an ontological structure instead of scientific knowledge describing discrete atomistic development of this nature [Bhaskar, 1978; Harre and Madden, 1975; Outhwaite, 1987].

In order to represent a whole world of design issues with human error (i.e. a concept of design-induced error), this research suggest an ontological approach by which we can

construct and understand their relation and issues(e.g. why the operators fail frequently to recognise the state of the system?) .. An ontological assumption is to search for what exists in a domain of interest. The reason for using the ontological assumption to represent a concept of design-induced error is that the concept is difficult to explain with logical methodologies (e.g. mathematics). It is better to pursue and show what kinds of entities exist in the concept (objects) and what are relations or process between them. Ontology is the concept of the structures of objects. Good ontology categorises relevant entities within the objects semantically.

This research tried to gather existing theories that would be composed of a concept of design-induced error. The category of a concept of design-induced error is based on theory. This is a kind of ontological method. Therefore ontology is a methodology as well as an objective in this thesis.

First of all it is necessary to know and define what is an ontology as used in this thesis. The term "ontology" terminologically is defined as: (1) a branch of metaphysics concerned with the nature and relations of being, (2) a particular theory about the nature of being or the kinds of existences (Webster's dictionary).

There are two aspects to the term ontology. From a philosophical point of view, ontology refers to the subject of existence, in which the content of a subject remains the same independently of the language used to express it. Ontology is a process of seeking a definitive and exhaustive classification of entities in all spheres of being in order to answer the question of what classes of entities are needed for a complete description and explanation of all the goings-on in the universe, which also include the types of relations by which entities are tied together to form larger wholes [Smith, 2003].

This aspect includes a study of the objects, properties, categories and relations that make up the world. Scholars in this area try to develop an abstract model or theory about the world.

The other aspect of the term of ontology is a model or definition of a world interest [Guarino, 1998]. People working in the fields of artificial intelligence (AI) or knowledge engineering use this aspect in order to develop knowledge-based systems. They say that an ontology is an explicit specification of a conceptualisation (Gruber, 1993), or a shared understanding of some domain of interest [Uschold and Gruninger, 1996].

Despite the differences between the philosophical (psychological or social) and technological application of the term, ontology is in general a methodology to represent a domain from which we can enhance our understanding of the domain as discussed

further in Chapter 8.

Sometimes *logic* and *ontology* are comparative concepts. Logic is only a system of rules for how to argue successfully, and ontology, as a categorical analysis and general theory of what there is, is a system of categories and laws about being [Cocchiarella, 2001]. Different approaches between "form-oriented approach" and "content-oriented approach" in artificial intelligence research illustrate a similar distinction of logics and ontology [Mizoguchi et al., 1995]. The former deals with logic and knowledge representation, the latter with content of knowledge.

Although a logical approach has achieved a great deal of advancement in AI research (e.g. expert systems) by developing powerful logical reasoning tools, it has been confronted with a difficulty over the fundamental issue of knowledge itself in current knowledge-management systems. It has nearly failed to answer a question about what is knowledge, what properties and relations a specific knowledge has. As a result, recently, research on ontology, which is a content-oriented approach, has come to gather much attention to tackle the problem that has not been solved by a logical approach.

Ontology is proposed here for that purpose. It is a research methodology that gives us a design rationale of a concept of design-induced error, a conceptualization of the world of interest, definition of meanings of concepts and relations in order to model the concept. It also provides an opportunity to share the knowledge captured in information systems.

This thesis uses the term ontology as: (1) a theoretical basis of a concept (i.e. design-induced error), and (2) computational conceptualisation of the concept that can be used in knowledge-based systems. Therefore this thesis will show two types of theory-based ontology of design-induced error.

The former is a theoretical ontology of a concept of design-induced error by which a meta-theory (i.e. an error inducing model) was constructed in Chapter 4. The meta-theory explaining human−system interaction failures can be used as an interpretation methodology of analysing such failures. The latter is a knowledge-based ontology (i.e. practical ontology) that is suitable in knowledge transfer in order to capture relevant knowledge from information systems (accident report systems in this thesis) developed in Chapter 7.

They intertwine with each other. The theoretical ontology helps to develop the knowledge-based ontology, and then the knowledge-based ontology helps to capture the concept of design-induced error in real accident reports.

3.2 Designing a research approach

A general process of a research approach (e.g. a general design research methodology [e.g. Blessing et al., 1995]) for developing a framework in many fields of research such as design, management, education, information, or psychological research follows:

- Identify question/raise issues
- Develop a model (or theory, hypothesis, propositions)
- Evaluate the model developed/analyse theory
- Analyse findings and confirm the model/discussion about results

The overall research steps employed in this thesis follows below:

Phase 1: Questionary studies stage: understand general human error models and characteristics of modern design concepts, identify phenomena that concern human errors and design problems with well reported accident cases.

Phase 2: Model development stage: introduce a concept of design-induced error, and develop a theoretical model (meta-theory) and an information model (ontology) of design-induced error.

Phase 3: Empirical study stage: select a test base of an accident report system, gather data from the accident report system, and screen out human error cases from the system.

Phase 4: Evaluation stage: analyse screened accident data with meta-theory of design-induced error, populate ontology instances with the data.

Phase 5: Discussion stage: discuss the result of analysis in previous phase, usefulness of reasoning tools, using search engine, recommendations to designers, accident analysis, and accident generating authority.

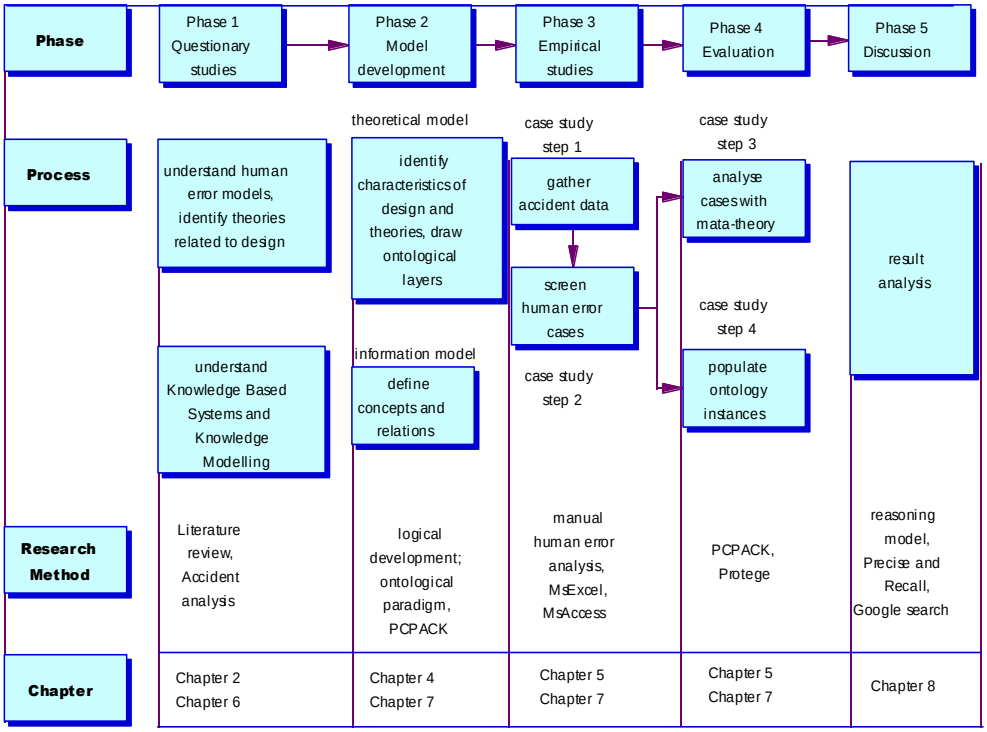


Figure 3.1 Overview of the research approach

3.3 Phase 1: Questionary studies

Phase 1 aimed to find out relationships between design and human errors. The findings from this phase helped to generate research questions and explore design issues in human error cases. The literature is mainly used to understand the current human error models and characteristics of modern design concepts such as automation, complexity of systems, and temporal decision making conditions. Accident cases have been explored, which were well analysed by researchers, that are considered as having design problems in connection with human–system interactions. Eighteen well-known accident cases showing design issues in human error were abstracted from journal papers, accident database systems etc. The findings from analysis of accident cases confirmed strongly the findings from the literature review; design can affect human operators adversely, but no correlation between the theories was identified.

3.4 Phase 2: Model development

As mentioned above there were two steps to develop appropriate models of Design-induced error that represent adverse influences of design to human cognition and performances; meta-theory of design-induced error, and ontology of Design-induced error.

3.4.1 Design of the development of a meta-theory of design- induced error

The main methodology of developing the meta-theory of design-induced error (design-induced error model) is an ontological method. The ontological methodology makes it possible to synthesise related theories gathered from the literature review and to categorise them in the light of a concept of design-induced error. The development of a theoretical model began with a literature review on human error and psychological theories that address design issues in human error. Case study (accident analysis) was conducted with well-known cases that raised design issues in human error in order to test the developed model. The process ended with constructing a new model (i.e. meta-theory) of design-induced error (Figure 3.2).

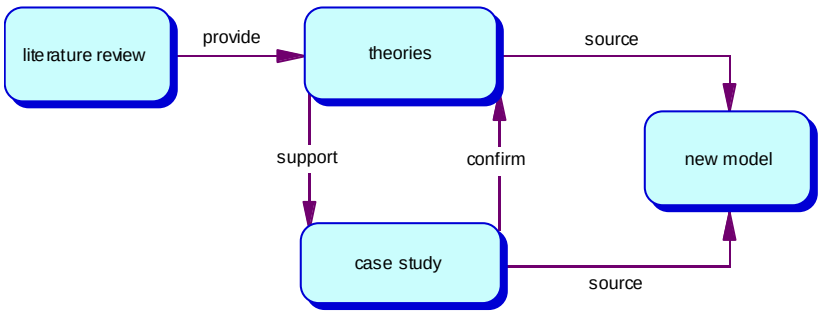


Figure 3.2 An overview of the development process of a theoretical model

The literature review on human error research was initiated from research questions (e.g. why some aspects of design of a system fail to help prevent users from making an error? and, can we create a new model that explains design issues in human–system interaction failures?). The literature review moved to find theories related to explaining design issues to human error. For the theoretical development of Design-induced error, a collection of related cognitive theories is an essential requirement because the failures of Design-induced error are based on limitations of human cognition and performance.

In order to develop and test a model, a case study was conducted as the next step. Case study means accident analysis in term of a concept of design-induced error. Conducting the case study had two parts. One is on cases found in the literature that was well explained with theory. The other part is a specific accident report system (the Australian aviation accident/ incident report system).

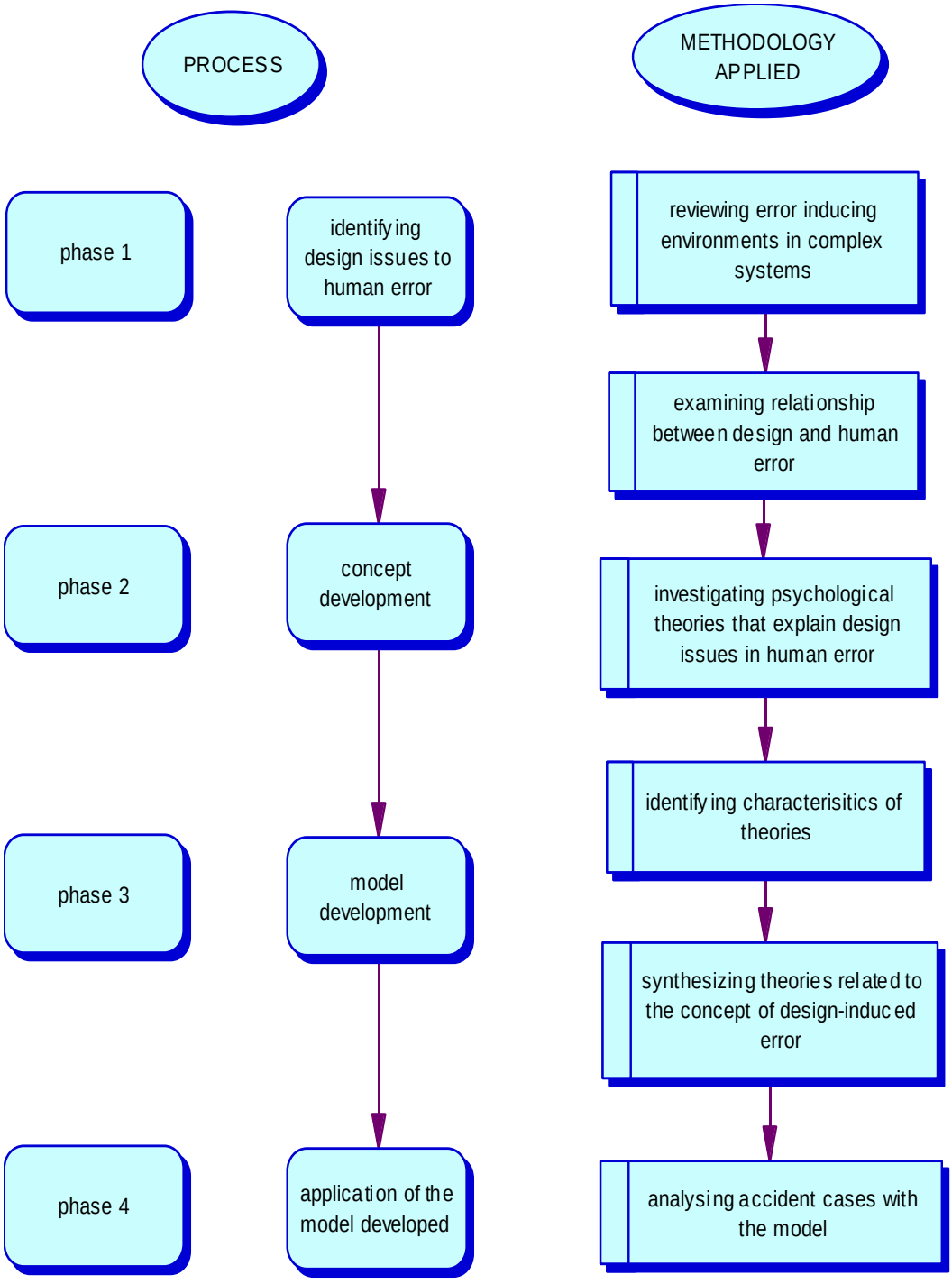


Figure 3.3 Development stages and methodology in theoretical model development of design-induced error

3.4.2 Design of the development of a design-induced error ontology for knowledge-management systems

As a practical approach, in order to develop a knowledge-based (KB) ontology we need to determine a specific domain to be analysed, carry out knowledge acquisition, and the knowledge modelling process (Figure 3.4). This process used methodologies used in web and hierarchical technology. PC PACK was the main technical methodology used in this process. The meta-theory of design-induced error defined in the previous stage was a theoretical methodology of analysing accident reports. An accident report system in Australian aviation accident reports found on the Internet was a knowledge domain for the analysis of the accident. The choice of ATSB is examined in Chapter 8.

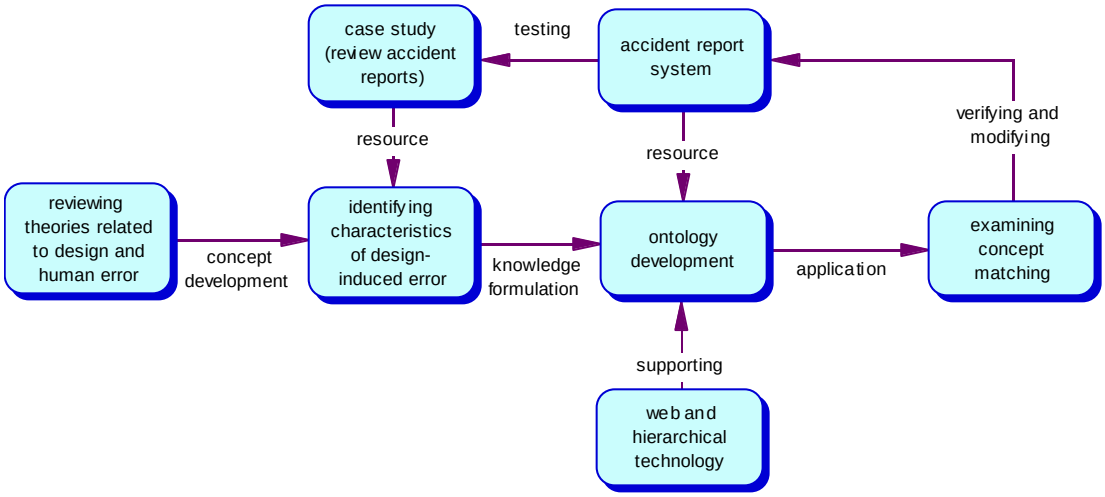


Figure 3.4 An overview of the development process of design-induced error ontology for knowledge capturing

The reason for choosing the PC PACK as a technological methodology is that PC PACK has a knowledge acquisition tool that makes it possible to extract knowledge from documents. It has also a web-publishing tool in which annotated (marked-up) documents can be categorised according to concepts. It is also compatible with Common KADS and MOKA that are used in an engineering domain.

In the development stages, in order to define the domain document set that contains the concept of design-induced error in a clear form, manual description analysis was adopted as a method. After extracting the document, PC PACK was used for the knowledge acquisition process, ontology template development process, knowledge

annotation, knowledge representation process, and web ontology browser producing process. Finally, in order to verify and validate the developed ontology, investigation was conducted on knowledge retrieval and representation reasoning support.

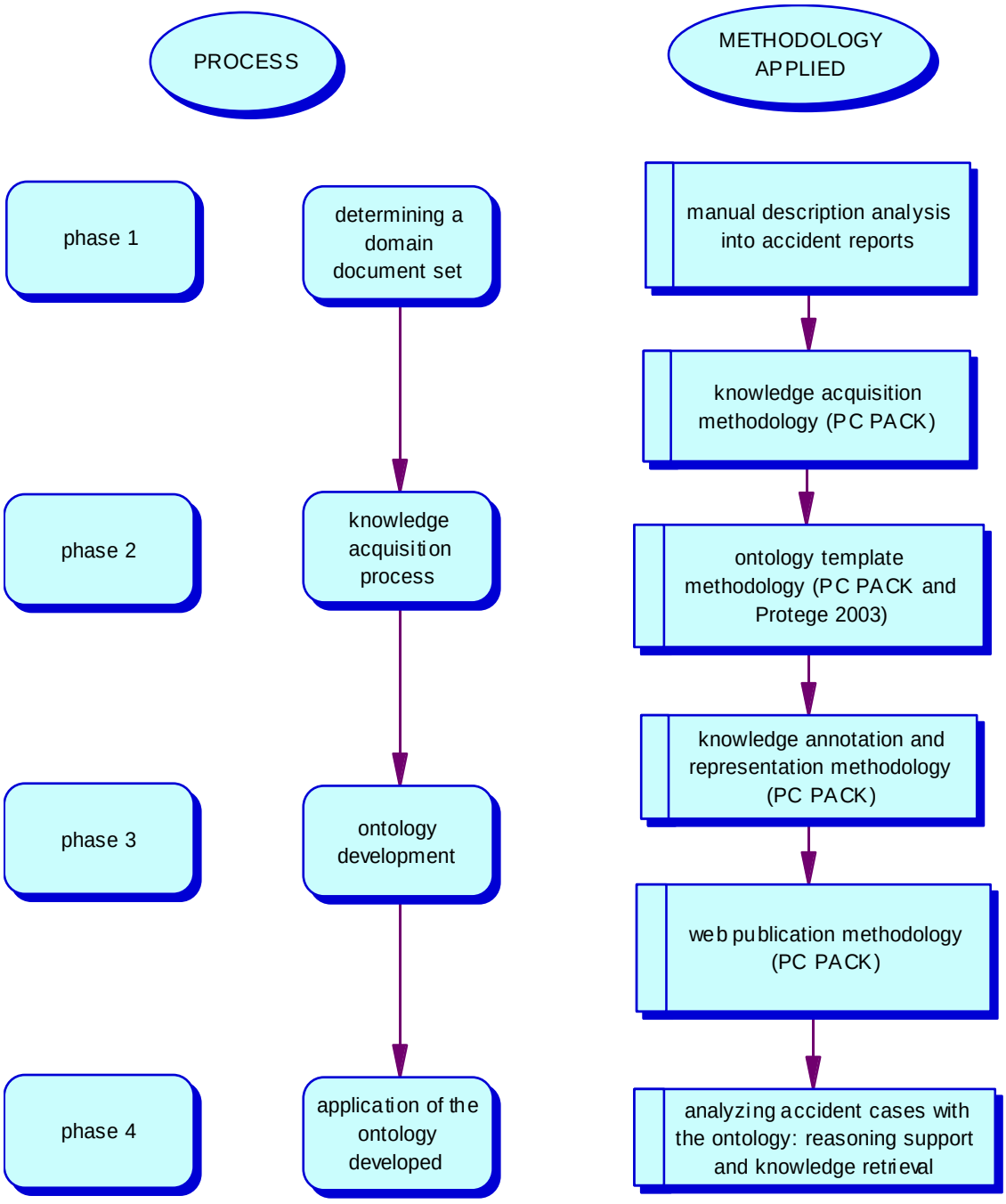


Figure 3.5 Development stages and methodology in practical model development of design-induced error

3.5 Phase 3: Empirical studies: accident analysis

Having developed models of design-induced error, it is necessary to test the developed models in real situations (accident cases, or human–system interactions). For this research, analysis of accident reports was conducted as an empirical study. This is a kind of case study in order to find various applications of models developed. How many cases containing the concept of Design-induced error are there in real accident cases? How does the model apply to accident analysis? Does this model make it easier to capture the concept than without the model?

It is not the purpose of this thesis to prove the rightness of models of Design-induced error. The model of design-induced error is based on meta-theory that reinterprets a theory with a new paradigm. Therefore theoretical proof is beyond the research because the main aim of the study is to find methods of application of theories.

Accident analysis case study using a particular accident database system was chosen to develop detailed and intensive knowledge about design-induced error and capturing the concept.

Choice of an accident database set

Analysis of accident reports is one of the most important sources for identifying contributory factors (Johnson, 2000). Many human-error researchers have devoted themselves to accident analysis. The choice of an accident report system as an empirical data set is a critical stage for achieving relevant research results. Which dataset is appropriate depends on the purpose of the research. The following are the main criteria to choose an accident data set:

- Rich information: Does the data contain much relevant information?
- Web-available: For developing a knowledge based system, it is necessary that the target data should be available on the Worldwide Web.
- Sizeable: A reasonable number of data entries is necessary to confirm the model. There is no fixed number of cases needed; however, a larger number may be more useful for data gathering and validation than a small number of cases.
- Easy to access or search: If the data cannot be analysed easily, it will be less well-known and take more time to identify or analyse.

The Australian Aviation Accident Report System (AAARS) was chosen as the empirical study of the research. By examining the criteria above, the AAARS was chosen as a better dataset for the study compared with other accident data systems.

Table 3.1 Comparison of aviation accident report systems

	AAIB	**AAARS**	**NTSB**	**CANADA ACCIDENT DATABASE SYSTEM**
RICH INFORMATION	Low	Very good	Good	Low
WEB AVAILABLE	Good	Very good	Good	Low
SIZEABLE	Low	High	Very high	Low
EASY TO ACCESS	Poor	Very good	Poor	Poor

Data collection: the data acquired from the AAARS was gathered into a Microsoft Excel spread sheet with ten categories. (Table 3.2, see Appendix A) 562 accident report cases, taken from the AAARS database were used Parts of the collected data which are considered as containing design issues in human errors were transferred into the Microsoft Access database program. Figure 3.6 shows a snap shot of the main view of MS Access program.

Table 3.2 Data tables gathered in the Microsoft Excel spread sheet

name of accident	date of accident	time of accident	accident type	cause of failure	cause of accident	failed system	defective artefact	failing system	improvement of system	design feature	type of operation at the accident	critical circumstance	trust on system	performance problem	defective cognition	cognitive experience
200302847	22-Jun-03	take off	ground	revealed no	exceeded the											
200304091	01-Oct-03	take-off	impact													
200403720	30-Sep-04	vehicle														familiar
200403210	30-Aug-04			then		fuel	gauges			gauges				not	ate fuel	different
200403210	30-Aug-04	abruptly												response		
200402749	26-Jul-04		from the	in a												
200305496	11-Nov-03	from runway	impacting the													
200404700	29-Nov-04	approach		delayed and		fuel quantity	fuel tank							subsequently	held senior	it had been
200402049	04-Jun-04											busy during			that fuel	
200404286	01-Nov-04		power cables	power cables											about the	
200402714	22-Jul-04	for landing		low' during												
200404460	12-Nov-04	through		n system was	hypoxic		following	went off the								
200401411	19-Apr-04	cruising level	a Cessna												that, as he	
200304918	30-Nov-03		the lower									and scattered	command	approach		
200302433	29-May-03	approach	approach			management										
200400443	08-Feb-04	training		ignition												
200303633	15-Aug-03	while	impact the													
200305203	17-Dec-03	for a	outboard													
200304938	27-Nov-03	selecting the		hydraulic	system											
200403868	11-Oct-04	take-off roll														
200304589	11-Nov-03		ground in a		and maintain											

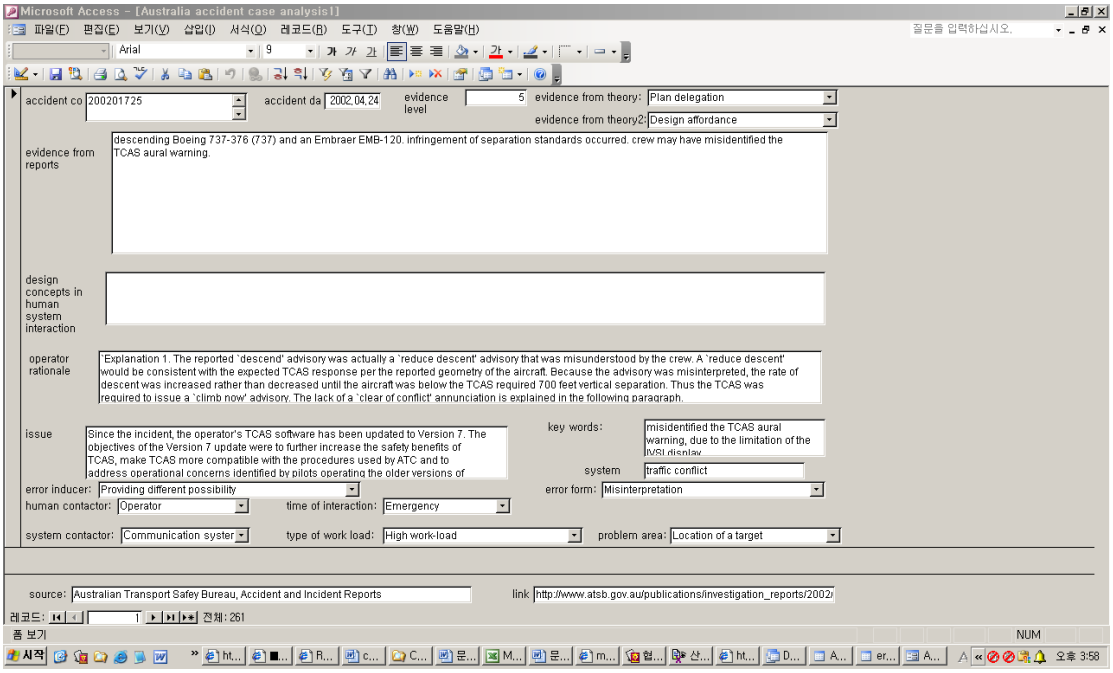


Figure 3.6 A snapshot of installed accident cases in the Microsoft Access database system

3.6 Phase 4: Evaluation

After finishing screening human error cases from other accident cases in the accident report system, evaluation processes were carried out to examine the usefulness of the developed models of design-induced error.

This research is not a pure quantitative research to validate the design-induced error by counting the quantity of captured numbers of accident cases. It is more important to develop a more understandable model to recognise issues involved in design and human error with the concept of Design-induced error. For the evaluation process, a qualitative research process was taken into account. Evidence representing the concept of design-induced error was examined in the process.

In order to evaluate the meta-theory of Design-induced error, the meta-theory was applied to the accident analysis processes. Out of a total of 562 accident reports, 287 cases were identified as human error cases. The author used a reasoning process (Figure 3.7) to identify related theories and an analysis sheet (Figure 3.8) to find different perspectives between designers and operators on design, which will be discussed further in Chapter 8.

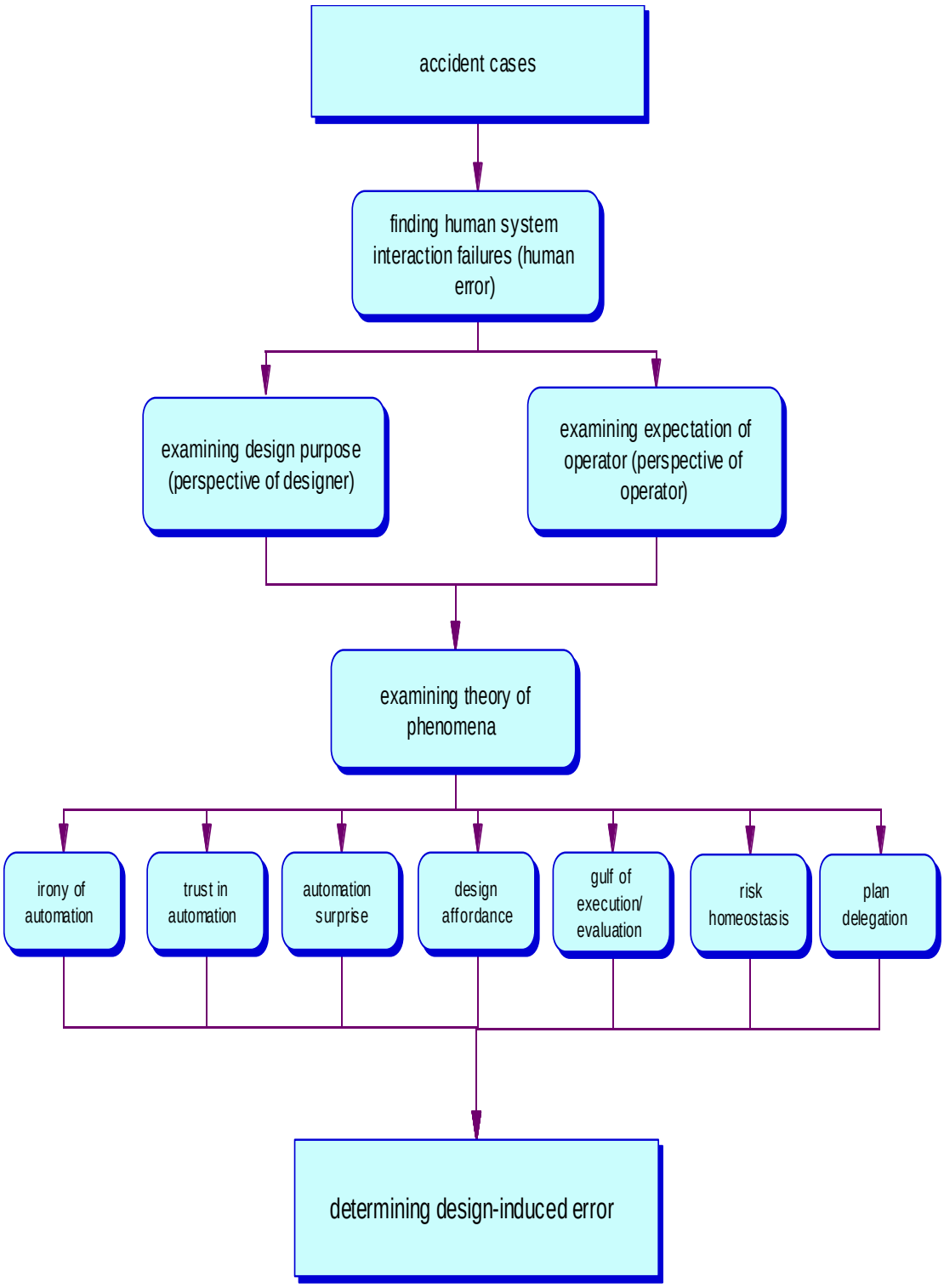


Figure 3.7 A reasoning process of the design-induced error model

Case number	
Accident description	
Human–system interaction failure	
Perspective of the designer	
Perspective of the operator	
Design-induced error	
Related theories	

Figure 3.8 An analysis sheet of human–system interaction failures in terms of design-induced error

When applying the meta-theory of Design-induced error to accident cases, the accidents were graded into five levels based on the evidence of the plausibility of Design-induced error. This process produced evidential terms and phrases related to design-induced errors that could be found in the accident documents.

Table 3.3 Levels of evidence for the design-induced error acquisition

LEVEL OF EVIDENCE	5	4	3	2	1
EXPLANATION	Strong	Good	Possible	Small	No

In order to evaluate the ontology of Design-induced error, Accident cases that were identified as containing design-induced errors in the previous stage were implanted. This process investigated how many attributes can be gained from accident reports. Diagrams were automatically produced by the knowledge acquisition program, i.e. PCPACK. This formed a small ontology of design-induced error ontology in aircraft accidents. This process produced instances of a Design-induced error ontology of aircraft accidents.

3.7 Phase 5: Discussion

The main aim of the research is to make models of design-induced error by which designers or analysts can understand adverse influences of design on human cognition and performance which lead to human errors. In the course of the evaluation process of the model developed in the form of meta-theory and ontology, in-depth qualitative feedback on the usefulness of the models was conducted. Firstly, the power of the knowledge model of the theoretical model was tested in the empirical dataset. Secondly, the knowledge model of design-induced error in information systems discussed how the reasoning model is effective to identify design issues in accident documents. Precision and recall ratio of concepts was tested using the Google search engine. Recommendations to researchers and accident reporting authorities in order to enhance accident report systems followed. Finally, future works and the limitation of developed models in this research will be presented.

3.8 Summary

This chapter has presented the methodology and research approach adopted in this thesis. The two kinds of ontological approach are the basis of the research. Table 3.5 summarises the research stages, methods and outcomes.

Table 3.4 Summary of research approach

RESEARCH PHASES AND AIMS	METHODS APPLIED	OUTCOMES
Phase 1: questionary studies -to raise research questions	− Literature review − Accident analysis	− Research questions formulated
Phase 2: model development -to develop models being relevant to research questions	− Identify characteristics of design and theories − Logical approach and ontological layers − identify concepts and relations	− a meta-theory of design-induced error developed − an ontology of design-induced error developed
Phase 3: empirical studies -to apply the models developed into real data	− Gather data from the Australian aviation accident report system (AAARS)	− human error cases in aviation accident reports identified − terms and phases describing the concepts captured
Phase 4 and 5: evaluation and discussion -to examine usefulness of the models	− Evaluation of captured cases with the theoretical model (V^2 analysis) and knowledge based information tools (PCPACK, Protégé, Google)	− The research questions answered − Recommendations to people concerned and identification of future works

Chapter 4. A Meta-Theory of Design-induced Error

In previous chapters the literature review provided an insight into understanding of human–system interaction failures. The characteristics of modern technologies that affect human cognition and performance and the role of design were also discussed. These issues were examined with accident cases. The theories can explain such issues well, but they are isolated from each other. It has been argued that we need a tool (e.g. a framework) to see a collective view on the theories. What is the underlying meaning of theories? How to link them? In order to tackle the problem, this thesis proposes a meta-theory of related theories. A meta-theory, a theory about theories is a broad perspective synthesising two or more theories [Ritzer et al., 2001], in this thesis is a framework for an integrated model of theories which describe design's influence on human error.

This chapter develops "a meta-theory of design-induced error" by proposing a contextual paradigm and an ontological assumption in which we can explain underlying structures of related theories taken from the literature review.

With these assumptions each theory can be organised in ontological layers and explained in terms of different perspectives between designers and operators instead of current scattered views. It can also help to identify design issues in human error accident cases.

There are several theories (perspectives) to bind in a form. Design-induced error is a highly complex phenomenon and to hope that a unifying grand theory will explain all its aspects is futile.

As a theoretical framework, a meta-theory will provide a possibility to combine theories. Firstly, it will articulate a set of ontological and epistemological principles that will help clarify the nature of design-induced error and our possible knowledge of it. Secondly, it will help bring together, in a logically consistent manner, some of the perspectives on design-induced error. In this way, the relationships between various perspectives will be clarified and, ideally, the scope of application of these perspectives will be specified. Finally, it will have an explanatory power to describe a human–system interaction failure with the local rationalities between designers and operators.

This chapter begins with summarising findings from the literature review (Section 4.1).

Which kinds of views on design-induced error are necessary for this research is discussed, comparing current views (Section 4.2). These findings were used as the basis of development of a meta-theory of design-induced error. A brief description of meta-theory is introduced in Section 4.3. Section 4.4 addresses development of a meta-theory of design-induced error with exploring the course of development of design-induced error, units of analysis, and factors that cause design-induced error. Finally, as a collective view of related theories, a meta-theory of design-induced error is suggested as one of contextual and ontological meta-theories (Section 4.5).

4.1 Findings from the literature review on design issues in human–system interaction failures

As summarised in section 2.6, theories of phenomena related to human error and design gathered and reviewed in chapter 2 are:

1) Gulf of execution/evaluation [Hutchins, Hollan and Norman, 1985]
2) Design affordance [Norman, 1998]
3) Irony of automation [Bainbridge, 1983]
4) Trust in automation [Muir and Moray, 1994]
5) Automation surprise [Sarter et al., 1997]
6) Plan delegation [Busby and Hughes, 2003]
7) Risk homeostasis [Wilde, 1982]

As reviewed in the previous chapter, the following common characteristics were drawn amongst the theories:

(1) They (theories) are talking about failures of design in human–system interaction.

(2) They address design issues relating to human error (e.g. design of a system introduces a condition in which operators can easily make an error).

(3) The problems addressed in the theories are not a direct and intentional failure of design but indirect and unexpected consequences of design.

(4) The operator could not comply with the operating specification of a system that was demanded or implied by its design.

From these findings it can be concluded that the theories of phenomena are concerned with "*human error that was induced by design (e.g. an operation of a system or a functional state of the system)*" especially in the currently prevalent automated complex systems. If a system left a human operator puzzling on solving a problem or managing an artefact in the system, such a system might be "an error-inducing system". This thesis names such phenomena as "design-induced error" in order to identify design issues in human error. Current theories explain well phenomena in which human operators suffer from mis-interaction with artefacts.

Each theory, however, has been developed to explain a particular phenomenon respectively. There is no theoretical approach to provide a collective view of the theories. In order to understand a whole area of indirect impact of design on human operators, it is necessary to recognise these theories together. An integration of these theories may provide greater understanding of these phenomena. Designers as well as accident analysts may have difficulty in knowing and applying all the theories. Providing a collective view of design-induced error can be beneficial to them.

4.2 Philosophy of Design-induced error

There are different views on the concept of design-induced error. It is important to decide on the kind of view of design-induced error for the research. This section reviews current views of design-induced error and suggests a new way that encompasses related theories.

4.2.1 Current views on the concept of design-induced error and the limitation of these views

… Identifying designs that can induce flightcrew errors having undesirable consequences early in the design and certification processes would allow appropriate corrective action to be undertaken at a stage when cost and schedule pressures are less daunting. In addition to the A320 FCU design, other examples where flightcrew error analysis may have identified design features that have been implicated in serious incidents or accidents are: flightcrew awareness that the autopilot is approaching its control authority (B747 China Air over the Pacific Ocean) and autopilot designs that allow pilot

> input to inadvertently create large out-of-trim conditions (A300-600 accident at Nagoya, Japan) … As stated earlier, flightcrew errors occur for many reasons and have many potential contributing factors. It is impossible to prevent all human error without removing the human flexibility and adaptability that contributes significantly to safety. Moreover, it is the negative consequences of error we wish to eliminate, not necessarily the errors themselves. However, it is still desirable to minimize errors that are design or system induced … The FAA should require the evaluation of flight deck designs for susceptibility to design-induced flight crew errors and the consequences of those errors as part of the type certification process.

[Federal Aviation Administration (FAA), Human Factors Team Report, 1996, pp. 96-7]

The quotation above demonstrates the importance of recognising a concept of design-induced error for designers to design a credible system. Design-induced error has become of particular concern of people in safety design domains because of the advent of modern complex systems [Salmon et al., 2003; Harris et al., 2005].

There has been frequent use of the term design-induced error since Meister's [1971] comment on the concept of design-induced error. Technology-induced error [Kushniruk et al., 2005; Borycki and Kushniruk, 2005] and system-induced error are used synonymously with design-induced error. The term design-induced error used in literature may be classified according to the following three points of view.

(1) Meister's view: classified errors as system-induced error, design-induced error, operator-induced error based on system development.

(2) Perrow's view: this opinion is about organisational considerations in the design process. Perrow argued that a design decision structure that affects equipment design is important to prevent system failures.

(3) Harris's view: focus on interface design, the most common concept that is well recognised by people.

These views show it is possible to define the concept of design-induced error according to different points of view. One is from equipment design point of view. This approach focuses on direct interaction between operators and systems (e.g. monitoring a display panel or managing a device [Harris et al., 2005]).

The other is from the point of view of error-inducing social/organisational systems [Perrow, 1983; Wagenaar et al., 1990]. According to this point of view, design-induced error is not a type of error rather it is one of the contributory factors that form human

error. There are several kinds of error- inducing factors i.e. organisational factors, individual factors etc. Design-induced error is considered as one of them [Meister, 1971]. It addresses organisational issues in order to tackle the problem of design failure (e.g. decision making process).

Limitation of current views on the concept are as follows:

(1) There is not a clear definition of the concept of design-induced error;

(2) Each concept address part of human performance and cognitive processes;

(3) Sometimes managerial or cultural issues are included.

Firstly, the concept of design-induced error has been used without clear definition. It is generally accepted that design can induce human operators to make errors in complex and automated systems. However, the concept of design-induced error has not yet been defined clearly. One reason not to define the concept clearly may be that it is difficult clearly to pick up the concept in human–system interaction failures among other factors contributory to the failure. The concept of design-induced error can be frequently compounded by individual or organisational factors. For example, a monitoring failure can easily be interpreted in terms of operator's haste or management demands, not design of the system. This circumstance may lead to concluding only training issues are involved, not design issues of the system.

Secondly, the current well recognised concept of design-induced error (e.g. Harris et al., 2005) is also limited to addressing all kinds of design-induced errors in every stage of human information processing because they mainly focus on interface design issues. Interface design, e.g. display in aviation control systems, is found in an execution stage of human information processing. Design-induced error can, however, be found in other states of human information processing such as a planning stage. For example, the theory of risk homeostasis points out that operators can fail to use a system correctly if the design of the system provides the operator with overconfidence in the safety of the system. Therefore, the concept of design-induced error related to interface design explains only some parts of the concept of design-induced error that would be formulated in this thesis.

Finally, a view that concerns organisational factors in the design process or design organisation should be excluded from the concept in this thesis because this research is focused on design itself. This research would not touch managerial decisions or organisational effects in the design process. Social or cultural aspects are also excluded in this thesis. However every system that is current is a socio-technical system [Busby and Hibberd, 2004]. As design of a system affects operators in the system socio-

technically, it should be considered in this thesis.

It is necessary to look at which stage of human information processing has relations with design areas and design-induced error. We can find design-induced error and design areas from the planning stage to the execution stage in human information processing as discussed later in Section 4.4.3..

4.2.2 Related Concepts

It will be useful to find characteristics of design-induced error if we compare other concepts related to error and design. There are concepts that can be compared with the concept of design-induced error. This comparison, however, will not try to scrutinise the definitions of them because they are not the main objectives of the thesis, but to find distinctions among them.

There are lots of other ways to categorise errors from different perspectives. First of all, one thing that needs to be mentioned is a difference from “design error”. The term “design error” may have two ways of being interpreted. First, with regard to who makes the errors, “design error” means “designer error”. When we clarify the error in terms of who makes the error, they can be categorised as designer error and operator error. The other way to interpret “design error” can be functional, constructional or process errors of systems in terms of the objective of errors. As a result, the error or failure from design error means the direct consequence of the design. For example, if the sign of a level-crossing is designed to show a “green” aspect instead of a “red” aspect when it needs to prevent passengers from crossing, the design can be called a design error. Design-induced error, on the other hand, the consequence of design, is not direct but indirect and it is difficult to notice the problem before the interaction failures occur.

Design specifications are important for designers. They are concerned about design requirements that meet rules and regulations. The wrong specification is a lack of requirements to meet demands in the current environment. On the other hand, design-induced error does not directly concern what is necessary for design. Design-induced error shows problems arising from design during humans tackling tasks in a system. Some knowledge gathered from concepts of design-induced error may be developed into design specifications.

This section chooses the concept of operator error and design error (engineering failure) as the main concepts comparable with design-induced error because they have

some common aspects with design-induced error. Error-inducing factors in the error-inducing model are also discussed in terms of the differences between them.

4.2.2.1 Design-induced error vs. operator error

Operator error is one of the most common types of error of many error classifications in accident and incident analysis. Design-induced error and operator error have similar and different faces (Table 4.1). It is not easy to distinguish between design-induced error and operator error because they have a same root, i.e. human error. However, it will be useful if we compare each and identify their different characteristics. They are all expressed through human activity. Sometimes it is not easy to distinguish one from another because they may be seem to be very similar. For example, operators can make an error by stress, by which operators' performance is downgraded in any task. The stress leading to the error could have arisen from design problems or from their physical weakness at the time of the error. In general, operator error has a broader boundary than design-induced error. It contains all aspects including design that affect operator's physical performances or cognitive processes. The concept of design-induced error concerns only about design issues, by which affect operator's performances during interactions with systems.

CATEGORY	COMMON	DIFFERENT	EXAMPLES
Design-induced error	Human error	Design related only	Misinterpretation of state of system by a poor design
Operator error	Human error	Including physical or emotional contributions of the individual	Misreading by fatigue, stress by an individuals' medical condition

Table 4.1. Distinction between design-induced error and operator error

4.2.2.2 Design-induced error vs. design error (engineering failure)

"Design error", sometimes called "engineering failure", is a main concern of every engineering project, whether mechanical, electrical, or architectural. "Design-induced error" and "design error" (engineering failure) have same origin – i.e. designers. They are all failures of design. However, the difference between them is their effects and

how these arise. Engineering failure affects artefacts resulting in direct and immediate failure, e.g. breakdown of a function to a system.

In the contrary, Design-induced error affects human operators (users) and as a result, the effect of the error would not be seen clearly in the system before the failure of human interaction occurs (Table 4.2). It may be said that a design error leads to a mechanical failure, and that these arise through normal operation. So a design error would not take into account the role of normal erosion that could be expected in the environment in which an artefact is used, or the handle to a door breaks because the designer did not take into account the forces that would act on it.

CATEGORY	COMMON	DIFFERENT	EXAMPLES
Design-induced error	Design related	Human error	Misinterpreting state of a system by wrong design
Design error (engineering failure)	Design related	Calculation error for endurance of artefact	Hardware failure- erosion, crack etc. software failure – computer programming bug etc.

Table 4.2. Distinction between design-induced error and design error (engineering failure)

A design-induced error would be the effect of the system on the operators' perception of it, which would lead the operator to use an artefact or the system in an unintended manner that could compromise the performance of the system. The question then arises as to whether design-induced error could be viewed as a subset of design-error, in that the designer has failed to take into account the characteristics of the operators, the social rather than the physical environment in which the system is used.

Therefore, design-induced error has both the nature of design error and human error that occurs in the form of failures in interactions between the user and the artefact in certain circumstances (Figure 4.1). It is caused by designed artefacts or design principles that typically have no effect on operator performance but which, under certain circumstances can lead to acute or chronic deterioration of operator performance, which can lead to active failure on the part of the operator.

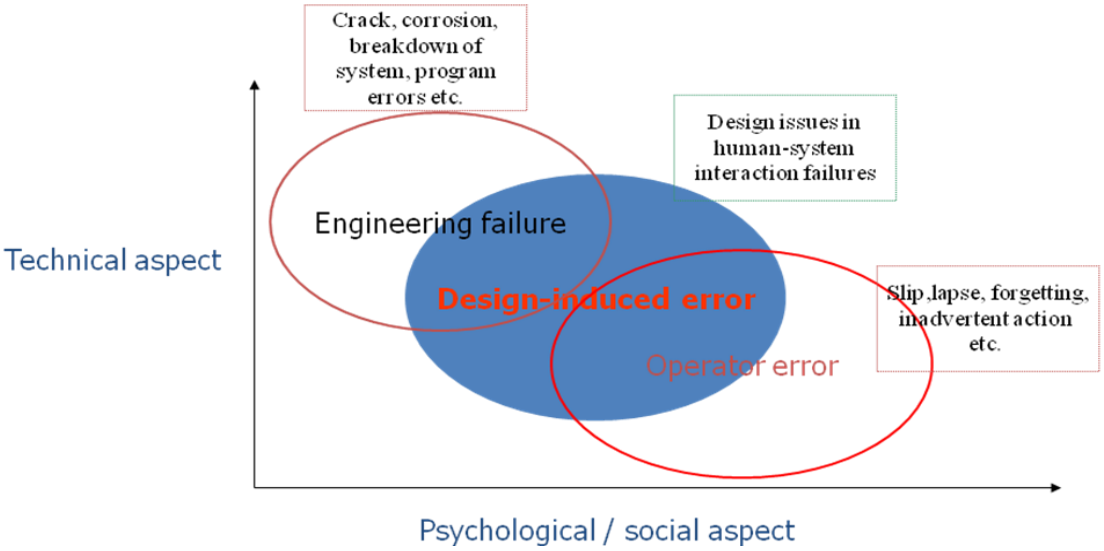


Figure 4.1. Location of design-induced error

4.2.2.3 Error-inducing factors

The other way to distinguish design-induced error from other concepts is by examining the concepts according to error-inducing factors. In the first section there are many error-inducing factors and they can be categorised into four domains in which errors can be affected and grown. According to Svendung and Rasmussen's socio-technical model (2002) an accident chain consists of a number of related stakeholders (see Figure 4.2).

The concept of design-induced error concerns design concepts, degree of complexity and automation, layout of instrument and signal design, and procedure design. The concept of management-induced error relates to management conditions such as demands of productivity, task pressure, work scheduling, allocation of operations, or relationship between managers and operators. The concept of culture-induced error concerns on risk perception in organisation or society levels, safety culture in an organisation, and collaborative (teamwork) conditions. The personal level of risk perception, inherent degree of personal vigilance or concentration characteristics, risk taking tendency, or habitual tendency are the main concerns of the concept of personality-induced error..

Comparing the technical aspect and cultural or training aspect we can divide the concepts. The concepts of design-induced error and management-induced error have more a technical aspect than the concepts of personality-induced error and culture-induced error. On the other hand, the concepts of management-induced error and culture-induced error have a high degree of cultural/training aspect in the concepts. Figure 4.3 shows 4 error-inducing categories.

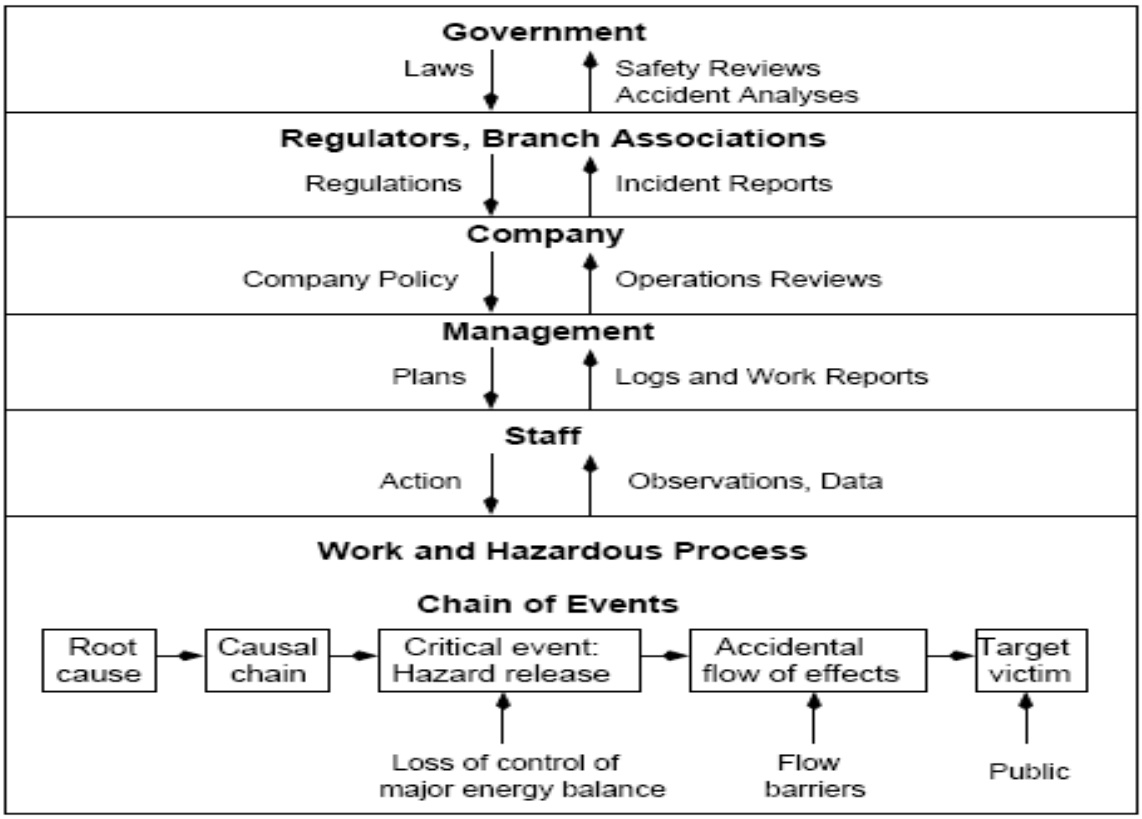


Figure 4.2 Rasmussen and Svedung's socio-technical model of system operations (adapted from Levenson, 2004)

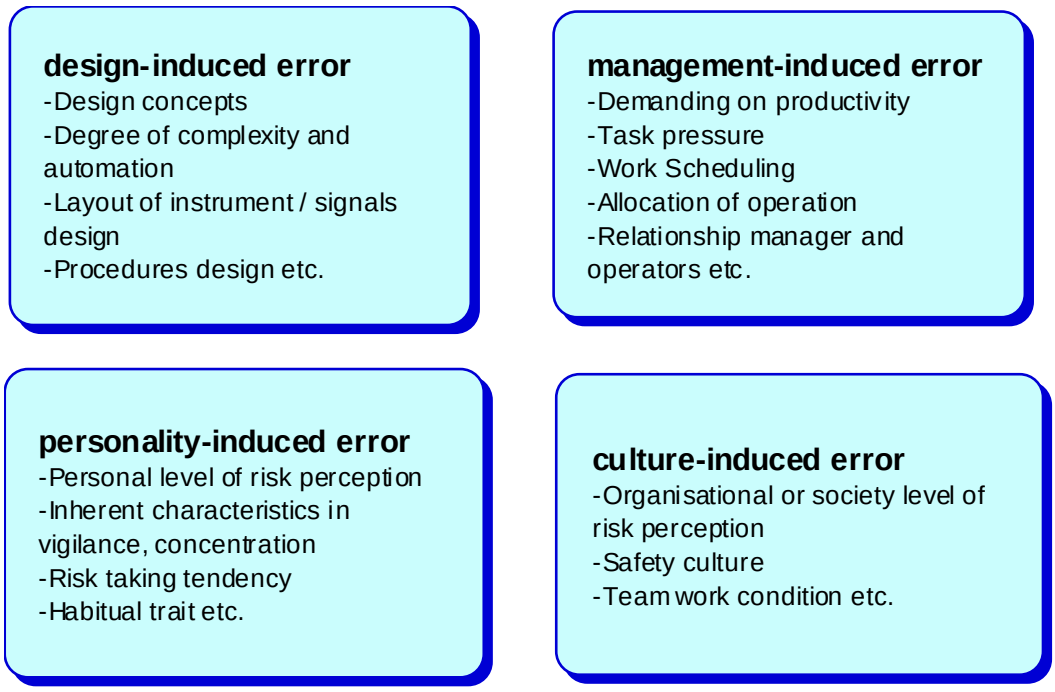


Figure 4.3 Different features in Error-inducing systems

4.3 Introduction to meta-theory

This section begins with an examination of two questions before turning to the development of a meta-theory of Design-induced error. Firstly what is meta-theory. Secondly, what we can do with a meta-theory of design-induced error. In general there are two reasons underlying the development of theories, approaches, and methods. The first reason is the evaluation of the truth of hypotheses about the world, often through logical manipulations of theoretical constructs, intuition, and thought experiments. The second reason is that people want to confirm their theoretical musings by empirical reference. Both cases require testable hypotheses to be validated or falsified, although this view is not shared by all [Shapiro, 1994].

This research is not to develop a pure psychological theory although its basis is in psychological theories of error. Rather, the aim is to develop a methodological tool (i.e. a framework) to see a collective view of related theories.

Therefore, this represents a meta-theory. "Meta theory" is a theory of (or about) theories. A meta-theoretical approach is a study about underlying structure, perspective, or philosophy of a theory (or theories). A meta-theory is underlying assumptions about what a theory is and influences descriptions, explanations, and predictions of a theorised model. In other words, meta-theoretical assumptions are those assumptions that underlie any given theoretical perspective. It sometimes is referred to as worldview. It is said that everyone has a meta-theory even if he/she is not an expert (e.g. a psychologist). A meta-theoretical approach can shape how we react to different explanations; and how we construct different explanations according to a particular paradigm adopted. Meta-theoretical assumptions subsequently influence our philosophy of developers (e.g. designers), how we learn and interact with others (e.g. users, operators). In a practical sense, an awareness of our own (and others) meta-theoretical assumptions allows us to understand better why we (and others) behave the way we do, thereby influencing (often positively) our future interactions. To a researcher of human error and design, an awareness of meta-theoretical assumptions allows for an understanding of the rationale behind many theories and research investigations, therefore providing a basis for a fair evaluation.

The value of any theory (including meta-theory) is not "whether the theory or framework provides an objective representation of reality" [Bardram, 1998], but rather how well a theory can shape an object of study, highlighting relevant issues. For example, a classification scheme is only useful to the point that it provides relevant

insights about the objects to which it is applied [Barthelmess and Anderson, 2002]. Halverson [2002] also identified four attributes that a theory as a tool for research should encompass such as description, rhetorical, inferential, and application power. The developed methodology can help people to analyse accident reports that contain information relevant to the concept of design-induced error and to extract semantic meaning from this information.

However, it is important to address here the aims and limitations of the development of meta-theory of design-induced error. As noted previously: 1) the aim of the research is to try to find a way of forming a collective view of existing theories of how design induces human error, not to replace them; 2) there is not one, unique meta-theory; 3) the function of the meta-theory is to help generate an ontology of the properties of design-induced error; 4) the purpose of the ontology of design-induced error is to help designers interpret reports of particular accident and incidents.

4.4 Development of a meta-theory of design-induced error

Theories related to design-induced error, using different theoretical understandings, have envisaged the reason why our interactions with a system or artefact fail. Design affordance theory mainly describes design issues at the skill-based level of our performance on an artefact. Gulf of execution and evaluation theory considers that responses and answers of a system to a user should be matched with the cognitive perception of the user on the representation of the system. Irony of automation theory concerns how automation has degraded the operator's abilities of problem solving and monitoring a state of the system. Trust in automation theory and automation surprise (or glass cockpit problem) raise issues on current digitalised automation systems that could be misunderstood or increase reliance of the operator on the system. Risk homeostasis theory addresses the idea that our belief in a safety system could be compounded by operators. Plan delegation theory shows that unclear allocation design can easily lead human operators to make errors.

This section presents the development of a meta-theory of design-induced error by examining underlying structures of theories in following issues:

- The course of design-induced error development (human–system interaction development)

- The unit of analysis (whole or (and) part of a system)
- Factors that cause design-induced error (causal conditions and determinants).

4.4.1 The course of design-induced error development

In order to understand an error process in theories it is necessary to investigate what kinds of interaction occur between a human and a system and which design elements are involved. By investigating theories, it can be derived that a system interacts with a human operator in the system by categorising different elements of the system. For the research design elements that consist of a system are categorised as; feature, function, logic, and reliability of a system. Human-system interactions are also classified in this thesis by three interaction levels such as affordance level, psychological logic level, and trust level according to human cognitive point of view. Figure 4.4 shows design elements and their relations according interaction levels. Each bar illustrates relationship between design elements with regard to interaction levels. For example, in an affordance level feature and function have relation in their understanding.

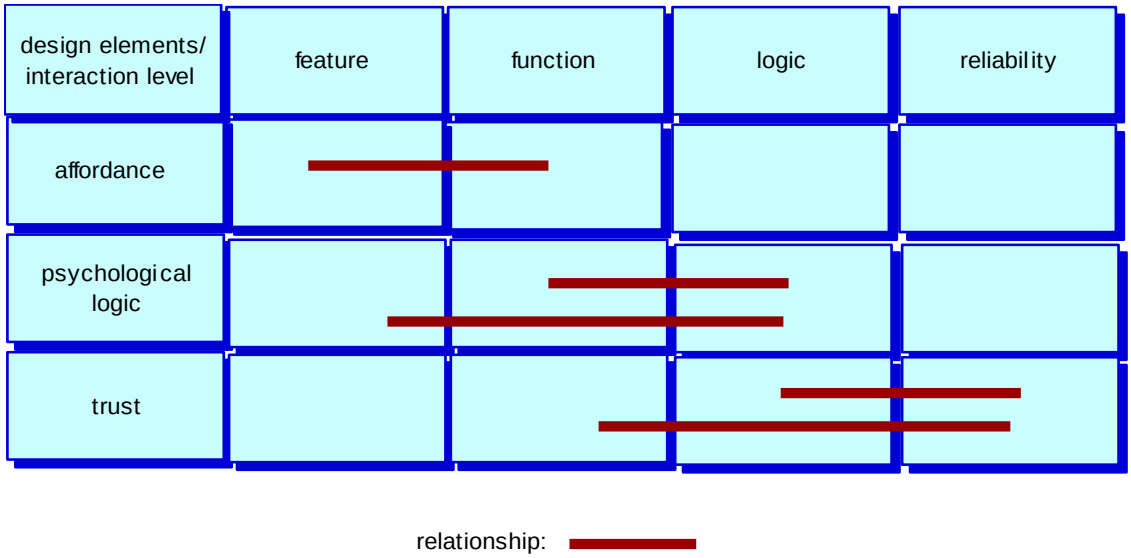


Figure 4.4 Relations between human-system interaction levels and design elements that constitute a system

A consistent connection between them is a necessity of a successful system. Feature refers to physical appearance of artefact like shape, colour, volume, or array of an

artefact. Function means what to do with an object: the purpose of on object. Logic means methods of working a system (e.g. a procedure); it is underlying principles of a function. Reliability means consistency of a system, not contradiction between lower levels of elements (e.g. logics) used in the system. The same systems should have the same logic, function, and features.

When we look at the course of human−system interaction in design-induced error, the system elements have connections each other. In general, feature has a connection with function, a function with logic, and logic with reliability of a system. Theories can be categorised with three perspectives according to connection failures among design elements of a system: an affordance level of Design-induced error; a psychological logic level of Design-induced error; and a trust level of Design-induced error.

In order to decrease or avoid cognitive overloads and to increase the efficiency of tasks employed, human operators tend towards lower levels of cognitive resources (i.e. knowledge-base to rule-base, rule-base to skill-base of performance). They use links between design elements by conceiving low levels of design elements for recognising higher levels of design elements. For example, a human perceives the purpose of an object by seeing a feature of the object.

In the case of cognitive breakdown of relations between design elements in human system interactions design-induced error may occur. It means inconsistence of relations of them is main course of design-induced error development.

Design affordance theory, an affordance level of perspective of design-induced error, explains a course of human error in terms of the relationship between feature and function of a system. Humans try to perceive a function of a system by recognising a feature of the system. For example, dials or toggle switches provide information of how to use them. When we watch a dial or a toggle switch we can immediately recognise its function of turning the dial or moving up/down the toggle switch by its feature of shape. If a feature of a system does not provide an affordable function, a user has a wrong perception of the function. It is an affordance issue of design. The upper part in Figure 4.5 shows that humans perceive artefact's function by feature.

In psychological logic perspective, a user's understanding process on the logic of a system depends on the function given to the user. For examples, in case of Therac-24 accident, the operators involved in the accident mistakenly pressed a button that radiate wrong voltage. Relevant theories are gulf of execution/evaluation, automation surprise, and plan delegation theory. The middle part in Figure 4.5 presents that a human understands a system's logics by its functions.

In the trust level of perspective of design-induced error, it is difficult for a user to organise all kinds of logic in a system that consists of the reliability of the system. As a result, the user relies on the system according to whether he/she believes in the system or not. Trust in automation, irony of automation, and risk homeostasis fall into this category. For example in the above Therac-25 accident case the system confused operators in a state of malfunction of the system because the system did not provide information relevant at that time. The low part in Figure 4.5 illustrates that human trusts system's reliability by its logics.

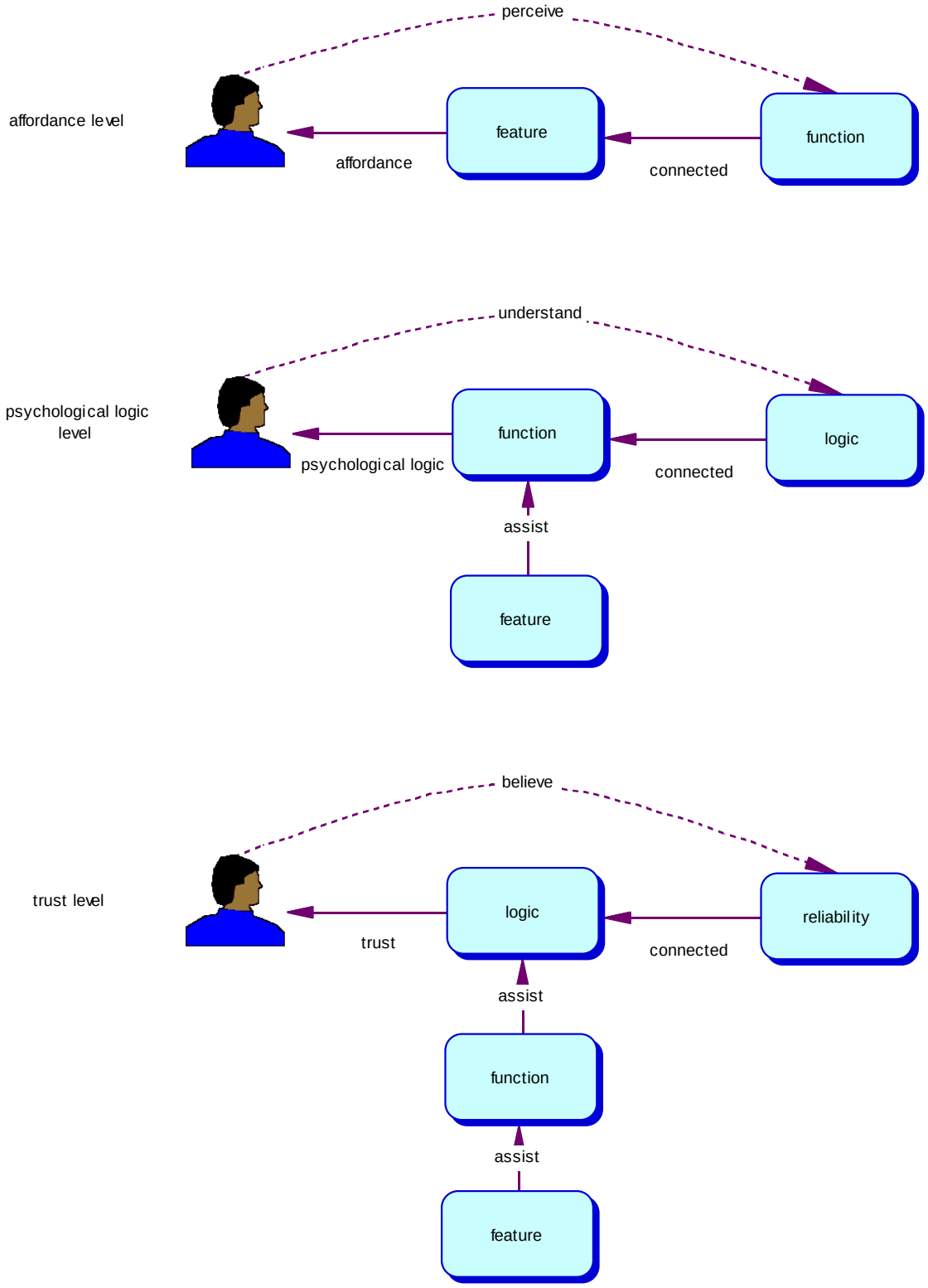


Figure 4.5 Three patterns of human–system interaction processes in order for human to figure out design concepts with design elements of a system

4.4.2 Unit of analysis I: Design levels in phenomena

If one wanted to study design-induced error, what would one look at? This is a question of the unit of analysis of design-induced error. For each of the theories, the unit of analysis differs. There are two categories of the unit of analysis in general: whole and (or) part.

Those who view design-induced development as direct human–system interaction argue that design-induced error occurs in interface (e.g., a monitor display). In other words, the development of design-induced error is assumed to occur in a process of direct interaction. For example, design affordance theory corresponds with the argument because the theory concerns what users contact physically (e.g. seeing an object). They can argue that design in design-induced error should be limited to equipment design (e.g. interface design).

On the other hand, those who view design-induced error development as a whole process of system operation argue that the development can occur in the human mind without direct interaction with an artefact. In other words, development is assumed to be a process in which ways of thinking, perception, and/or behaving emerge at specific times (stages) in a system. They argue that the boundary of design in the design-induced error process should be expanded into socio-technical system design. Irony of automation theory, for example, needs operators' interaction with a system to be extended to the whole system design concept.

It is necessary to determine the boundary of design in this research in order to define the concept of design in the meta-theory of design-induced error. There are many different views of design concepts in research (Table 4.3). To what extent can design concept to be applied in this research? Engineering designers tend to consider that the issues of design-induced errors are problems about physical systems and their direct interaction problems with operators during operations only. A socio-technical point of view, on the other hand, broadens the concept into organisation and society.

Table 4.3 Different views of concepts of design

System	Design
Society	Sociological design
Organisation	Managerial design
Communication and scheduling of operation	Logical, psychological design
Procedures, rules, manual	
Architectural system	Physical design
Component of artefact	

The terms "design" and "system" are considered as they have different definitions and are used differently according to research applications. Design is not only concerned with a physical system but also logical, psychological and social aspects. Design consists of concept, methodology and methods (Table 4.4). A "system" is a physical form with procedures in order to achieve particular purposes. The system is constructions of design concepts and methods. Humans achieve their goals through the system.

LEVEL OF DESIGN	ERROR INDUCERS IN DESIGN	EXAMPLE OF DESIGN-INDUCED ERROR
Conceptual design (High level)	A concept forming a system in order to achieve a goal of the system does not match with human cognition and performance behaviours	Misunderstanding a protection system
Methodological design (low level)	Methods used in a system do not help human cognitions and performance to do a task	Misreading a number in a display panel

Table 4.4 Levels of design concepts

Therefore, the concept of design-induced error can also vary according to the concept of design applied (Table 4.5): narrow concept and broad concept of design-induced error.

- Narrow concept: focus on direct interaction problems between human and system, i.e. errors that appear while human and system actively exchange their information and activities.
- Broad concept: expand into all human−system interaction problems including social factors such as organisational or managerial factors.

Research into human factor is the study of the multiple interactions between the human, the tools they use (from simple everyday products to advanced technologies), the task, the workplace, the environment and the organisation, and the application of resulting knowledge to understanding (and improving) these interactions [Noyes, 2004].

For example, in the case of the rail collision accident at Ladbroke Grove in London in 1999, it was suggested in the report of this incident that the cancellation of the AWS could have been an automatic response [HSE, 2000]. The AWS warning does not distinguish between caution and stop aspects. On the approach to a major station, such as Paddington, the volume of traffic means that many of the signals that drivers encounter would show caution aspects. As a consequence, drivers cancel AWS warnings on a regular basis, which could lead to a potential automation of their response. In this case, the driver may simply have mistakenly believed that the AWS warning at signal SN109 indicated that it was possible to proceed. To address the problem in this case, it is necessary to understand working conditions surrounding the driver as well as the artefact itself that interacted with the driver. Therefore, in order to tackle the issues arising in design-induced error, designers have to know the conditions surrounding operating systems, i.e. socio-technical conditions that affect use of artefacts and systems.

Design has increased the allocation of tasks for operators to do, tasks which must be performed nearly simultaneously, or without previous information, in modern complex systems. This was not a serious issue in a simple system. However the increased tasks with more complexity, mostly procedures, are now too constraining for human operators. Therefore many of the procedures should be solved by design.

The concept of design in this research should be expanded into indirect interaction problems i.e. design of procedures, rules and communication produced by designers. The term “design” in this research contains principles and expressions of designers to

construct a system: (1) methodology of system formation, function, (2) operating principles of systems, (3) mechanism of works, (4) methods of task process and procedure, (5) logical explanation of interaction among systems and operators, and (6) the representation methods of tasks and procedures.

Table 4.5 Comparisons between narrow and broad concepts of design-induced error

	NARROW CONCEPT OF DESIGN-INDUCED ERROR	BROAD CONCEPT OF DESIGN-INDUCED ERROR
Research purpose	− Finding design problems in direct interaction between human and system in interface design	− Finding design contributions and protective measurements of design in all human−system interaction failure in terms of design perspective
Advantage	− Explaining the problems in detail − Easy to understand the causation of error	− To explain many human errors in terms of design aspect − To understand indirect relationship between design and error
Disadvantage	− Too limited concept − Not to recognise design problems related to indirect consequence of human−system interaction	− Easy to be too wide concept − Difficult to distinguish from general human error study

4.4.3 Unit of analysis II: Human−system interaction stages in phenomena

According to Rasmussen's step ladder model of human information, process flows from activation to execution [Rasmussen, 1993]. This idea has been adopted in many domains such as chemical processing, nuclear power generation and aviation. He suggested that systems should support each of the different stages of information processing. For this research positions of phenomena on each stage of the human information process according to their influence were located. In which information process they (phenomena) are (or affect human cognitive processes)? It has been

attempted to identify at which stage in the operator's information processing each of the phenomena has its effect.

Risk homeostasis is located in activation and observation stages because before people exploit a system they are seized with a thought that a protection system will exist. Therefore, it happens just before or immediately upon observing a real danger or hazard.

In irony of automation, operators recognise the problem in the stages of observation and identification. They are alerted that there are problems from systems. However, their ability to deal with the problems has degraded they can only observe and identify, they do not go further with actions.

Trust in automation occurs through observation to interpretation. Operators observe and identify what is going on, but it is not based on correct interpretation. They just believe or not the state of systems. Therefore, their interpretation is based on trust in automation.

In glass cockpit problems, an operator's observations and interpretations based on glass cockpit displays were mediated by the sometimes incomplete mental models held by the operator. Therefore, their evaluation of the state of systems is vulnerable to error.

Gulf of execution refers to the difference between intended action and the actions that the operator believes that the system will allow. It is important that a capability of design might exist but that this might not be apparent to the user from the user interface. Also, the gulf of evaluation refers to the amount of efforts that the operator has to invest in deciding what the state of the system is. The gulf of evaluation also refers to whether the operator can interpret the state of the system from presented information, which might not be the case [Norman, 1988].

Plan delegation arises when users recognise that artefacts are prepared for a particular task. For instance, when an operator starts an engine he or she evaluates and defines the engine as prepared for the job. However, when the engine is expected to pre-diagnose some functions itself, they fall into plan delegation. Therefore, the user's procedure on the task cannot be correctly conducted.

Design affordances exploit unconscious processes of cognition. For example, when we see a chair we can just sit down on the chair without any decision reasoning process. Therefore, the problem of design affordance occurs in the stage of procedure and execution.

Table 4.6 depicts where phenomena are located in human information processing. It

illustrates where phenomena are placed throughout the information process. It means that the designers have to consider all stages of the information process while designing system tasks.

	ACTIVATE	OBSERVE	IDENTIFY	INTERPRET	EVALUATE	DEFINE	PROCEDURE	EXECUTE
RISK HOMEOSTASIS	X	X						
IRONY OF AUTOMATION		X	X					
TRUST IN AUTOMATION		X	X	X				
AUTOMATION SURPRISE		X	X	X	X			
EXECUTION/EVALUATION GULFS			X	X	X	X		
PLAN DELEGATION					X	X	X	
DESIGN AFFORDANCE							X	X

Table 4.6. The stage of information processes according to phenomena of design-induced error (modified from Rasmussen, 1983)

4.4.4 Factors that cause design-induced error: Local rationalities between designers and operators in phenomena

Accidents examined in chapter 2 show that the design-induced human errors occurred in a condition of temporal decision making environments. Complexity of the system contributed to this environment. Therefore, it is pointed out three factors as causal factors of design-induced error; complexity of a system, temporal decision-making condition, and local rationalities between designers and operators.

The previous chapter 2 described two factors (i.e. temporal decision-making condition, complexity of a system) as major factors that affect human cognition processing. Temporal decision-making condition and complexity of a system provide increased roles of a system in human–system interaction in modern systems. This section mostly discusses local rationality.

If we agree that in modern system environments the existence of temporal decision-making conditions and complexity of a system is inevitable, there remains a fundamental question why design of a system has not always coped with failures of human–system interaction. Although, the designer has abilities to create such complicated systems with modern technologies and logics, a number of reports of human–system interaction failures show there is lack of good design knowledge in the interaction.

Engineering designers may not recognise well how their designed systems are used by human operators because human cognition and behaviour are not their main concern in designing the system. It is said errors may result when the demands the system design places on the user exceeds their capabilities. A discrepancy between human mental resources and a system's demands can cause errors [Rasmussen, 1986]. Therefore, design-induced error is a consequence of the mismatch between designers' and user's mental models. Busby and Strutt [2001] illustrated how and what kinds of different perspectives designers and operators of hazardous installations may have.

Norman [1988] illustrated the different rationalities that exist between designers and users with regard to the operation of a system (Figure 4.6). When there is an artefact, designers have one concept of system(A) and rationality(A), whilst users form another concept that means system(B) and rationality(B) (Fig. 2). This is called local rationalities. It is suggested that these local rationalities arise because there is poor exchange of knowledge between designers and users.

Woods and Cook [1999] argued that consideration of the local rationality of operators such as resolving conflicts, anticipating hazards, accommodating variation and change, coping with surprise, working around obstacles, closing gaps between plans and real situations is critical for the development of safer systems.

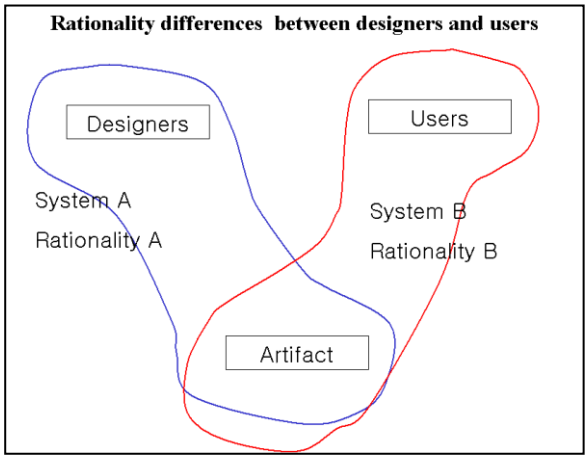


Figure 4.6. Local rationalities between designers and users (from Norman, 1988)

From this perspective, design-induced error may be generated from as the inconsistencies in local rationalities that exist between designers and users. Designers' misunderstanding about operators induces inappropriate design of the artefact and system. For instance, in the Three Mile Island nuclear

power plant accident in 1979, operators failed to recognise that the relief valve was stuck open because the indicator on a control panel misled operators. The light (valve indicator) only showed the state commanded for the valve, but not the actual state of the valve [Reason, 1990].

Therefore, the causes of design-induced error are determined by how designers consider operators in terms of discrepancy of local rationality: (1) Designers do not well understand the operator's cognitive performance. (2) Designers do not well understand the fact that operator's cognitive demand is increased when in an abnormal situation and do not function at the dynamic moment. (3) Designers do not fully understand the fact that a system is not perfect and has inherent deficits causing errors and failures, in that situation, there is a need for the involvement of human operators to handle the problem, however, designers do not provide information on the state of the system and cues of that.

4.5 A Meta-theory of design-induced error

Previous sections examined the underlying structure of the related theories and what is (or would be) design-induced error in order to provide a basis (i.e. meta-theoretical assumptions) of a meta-theory of design-induced error. This examination revealed that each theory has different perspectives. For a meta-theory of design-induced error, in order to encompass all related theories, the following assumptions for a meta-theory of design-induced error are suggested:

(1) Human operators have interacted with a system environment resulting in developing their own perspective on the system operation (Section 2.5.1);

(2) The design of a system creates the system environment in accordance with the perspective of the designer of the system (Section 2.4.1, 2.4.2);

(3) When the operator has a different perspective on the system operation from the designer, design-induced error occurs in certain circumstances (Section 2.5.3);

(4) Human–system interaction in a system includes socio-technical interaction (e.g. trust in a system) (Section 2.3.3);

(5) The concept of design in design-induced error should concern not only equipment design but also system design such as manuals, and procedure design (Section 2.5.5);

(6) Each theory is understood to occupy one position on the ontological layers of the meta-theory of design-induced error (Section 2.6.2, Section 4.4.1).

(7) The existence of a local rationality between designers and operators is regarded as a determinant of design-induced error. The relation between causal conditions and a causal determinant decides an occurrence of design-induced errors (Section 4.4.4).

A system environment, in this thesis, means all sorts of environments created by design of a system, which an operator meets while operating the system. For example, while an operator is conducting one task, there remain other planned tasks, procedures or processes of the system that lead to haste of the operator, constituting the system environments surrounding the operator.

Table 4.7 summarises the elements of a meta-theory of design-induced error and its assumptions. With the assumptions we can interpret related theories in the meta-theory of design-induced error. This is a contextual and ontological meta-theory. From this approach we can see a collective view of related theories.

An ontological assumption assumes the related theories consist of whole phenomena of design-induced error. Each theory is, as a result, a part of a category of design-induced error. It is assumed to have three different perspectives layers.

A contextual paradigm of design-induced error, which is based on a distributed cognition theory, assumes that the course of development of design-induced error is both a technical and psychological (and social) process in a system. In addition, the individual (i.e., human operator) and the system environment are both assumed to be active participants, reciprocally influencing each other. Development of design-induced error is best understood through examination of the whole as well as the parts. Metaphorically, the contextual meta-theory can be symbolised as a tennis game.

ELEMENTS OF THE META-THEORY	ASSUMPTION
The course of design-induced error development	Three ontological perspectives layers of human−system interaction
Unit of analysis	Whole and parts of a system
The causal condition of design-induced error	Complexity of a system and (or) tasks Temporal decision making condition
The causal determinant of a design-induced error development	Local rationality between designer and operator

Table 4.7 Elements of the meta-theory of design-induced error

This view assumes that both the cognition of a human operator and the system environment (i.e. design) are active participants in design-induced error. Additionally, influences are assumed to be reciprocal. This notation can be read as "large contributions from the system environment as well as human operator, where both are actively influencing the other". In this paradigm design-induced error refers to an imbalance between the reason of a system (i.e. intention of design) and the expectation of operators.

Figure 4.7 shows a model of a meta-theory of design-induced error. In this model each theory might be explained using the concept of local rationalities.

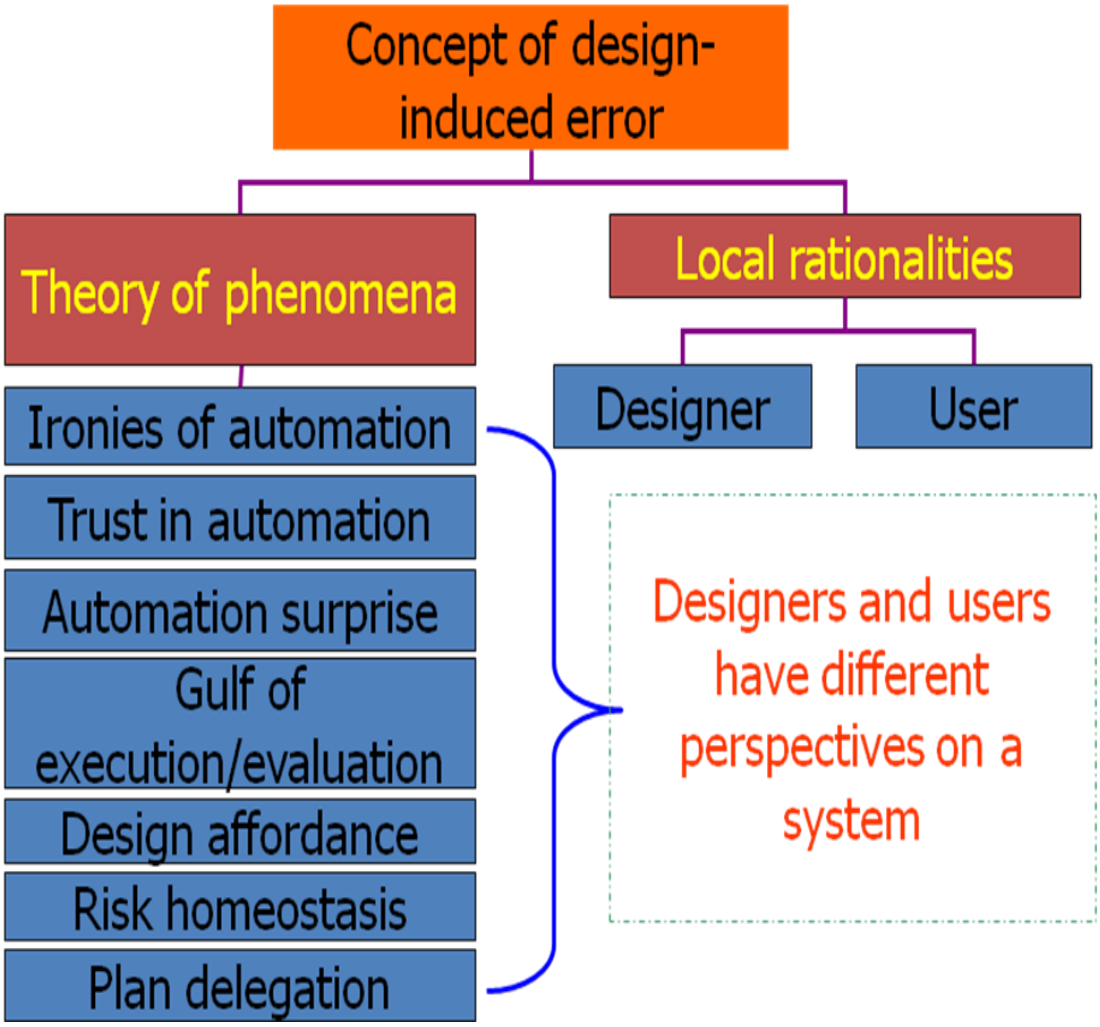


Figure 4.7 A model of a meta-theory of design-induced error

4.6 Ontological levels of design-induced error

This thesis proposes a design-induced error model in three levels of ontological layers in order to encompass all sorts of related theories. This model is to conceive of design either in abstract and indirect activities of a system and the operator in a socio-technical system level, or as an equipment design level that just represents physical artefacts.

① **Affordance level**

② **Psychological logic level**

③ **Trust level**

The three ontological levels of design-induced error bind theories interconnected within

the layers. From the surface of a system, which is more related to physical level of design, to internal operation of a system, which is more concern about conceptual level of design, we can understand phenomena in a collective view. Figure 4.8 shows ontological layers of difference perspectives of design-induced error. When we move from an ontological level to other level (e.g. OL3 to OL2) design level and phenomena of design-induced error are changed to more conceptual level of design.

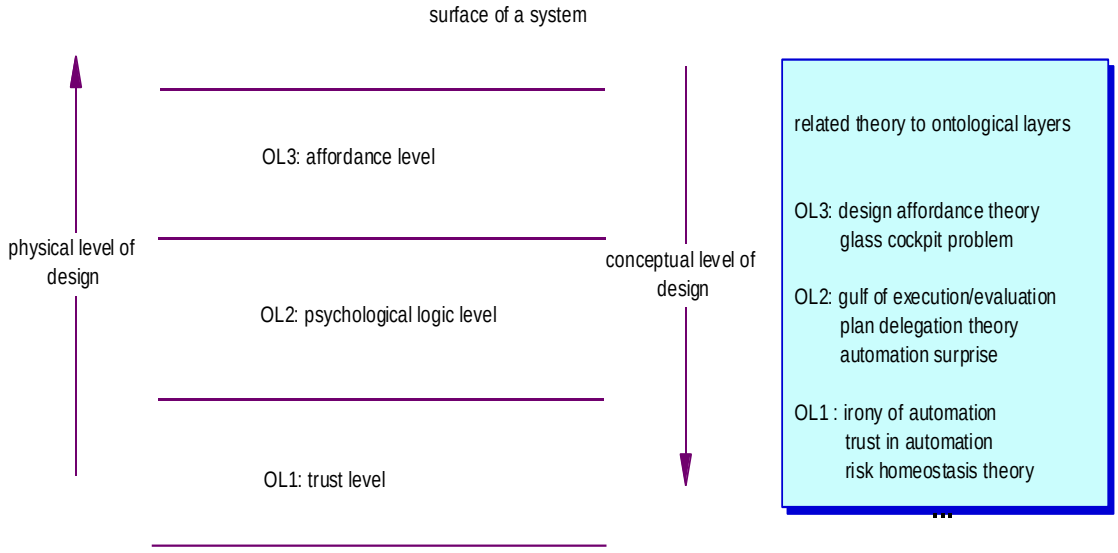


Figure 4.8 Ontological layers of different perspectives of design-induced error

Theories that were previously found in the literature are linked with these layers (see the box in Figure 4.9). They have been arranged in the ontological layers of design-induced error (i.e. OL1, OL2, OL3). Different layers show different connections between system elements. Deeper theoretical descriptions penetrate further down into the object of study and capture new layers. Moving from a phenomenon located at a particular layer to the layer immediately below it reveals the conditions in which the phenomenon under study is made possible.

Firstly Affordance level (OL3) is a study of errors related to behaviour identified with positions and shapes of artefacts. It has attempted to deal with the directly observable practices of design-induced error in carrying out their tasks within specific design (e.g. computer interface design). Its perspective comes from the equipment design point of view. This type of study is certainly valuable in offering us a picture of what design of

feature of an artefact means to the operator, and any further research at this layer will have to deal essentially with the connection between feature and function which are systematically associated with how a particular feature has a link to a function for a human. However, if our description of design-induced error is restricted to the surface level (i.e. a direct interaction with an artefact), we are forced to ignore or misunderstand other types of design-induced errors that occur gradually over a long time. There remain still other relations between different elements of design. For more descriptions of design-induced error hence we need for deeper theoretical descriptions.

Psychological logic level (OL2): What are the role of function and logic in a design for human operators? We need to move to a deeper layer of design-induced error to answer this question. The psychological logic level of perspective on the nature of design-induced error provides some answers. This view is partly from a system point of view and partly from an equipment point of view. For instance, the gulf of execution and evaluation theory noted by Hutchins et al. [1985] gives examples about certain functions that are different from the expectation of operators, causing operators to be puzzled in their attempts to recognise the logic of the system. A function provided by a system should be matched with cognition of operator as psychologically relevant. Similarly, the design concern with both continuity and innovation that has been emphasised by Sarter et al. [1997] implies the existence of roles such as resource allocation and disturbance handling. As will have, hopefully, become clear by now, the reasoning behind this analysis is that for particular design roles to be possible, a certain configuration of design tasks characteristics must be in place.

Trust level (OL3): Finally, how can we humans recognise the reliability of a system? It is nearly impossible for a human operator to check all possible conditions in a system; especially hectic, modern, complex systems that push operators to do tasks without any delay. As a result, operators have to depend on information provided by the system. A concept of design-induced error considers such conditions also. In order to answer the question above we should consider the nature of design, by locating design into its socio-technical context and conceptualising the manner in which this context endows design with abilities. The abilities attributed to design reside in the domain of the real and are not directly observable in the empirical domain (OL1). This is a whole system point of view that considers socio-technical system condition. For example, the question arises of how a human operator continuously monitors a display? The risk-homeostasis theory perspective on design has emphasised the balanced and cooperative control design of a system in preventing the transformation of an operator reasoning system into an inappropriate trust system in the context of contradictory relations of tasks. The excessive concern on a partial system, without consideration of a relation in

a whole system makes it easy to commit errors by the operator in the system. It is necessary to study capabilities of design that are not prescribed, but may be conceived by the operator in relation to other parts of the system.

The ontological structure can provide answers to questions for a meta-theory of design-induced error such as: How to connect different design perspectives for design-induced error? What kinds of design that are capable of committing design-induced error exist? When design-induced error occurs, what is a state of the system in that occurrence?

The following diagram in Figure 4.9shows how a theory can develop other theories by moving from one layer to another layer.

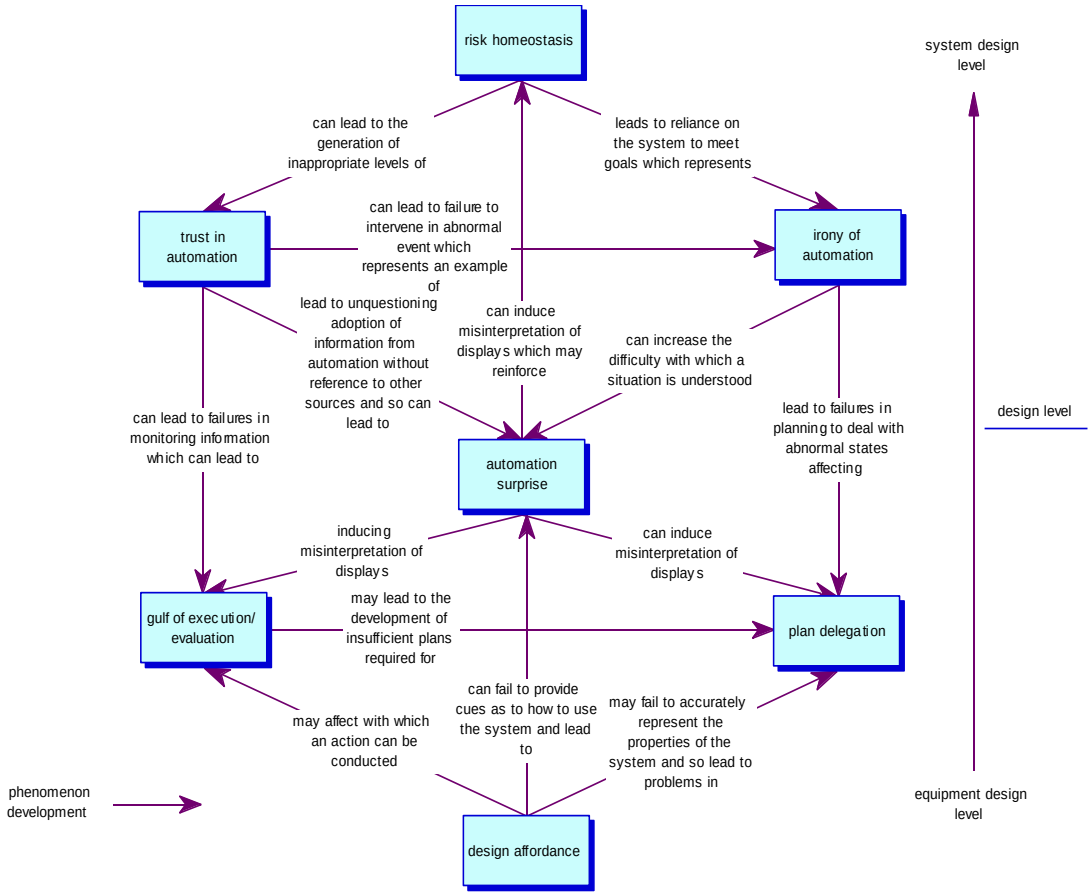


Figure 4.9 Phenomena changing between design-induced error theories according to levels of design concepts

4.6.1 Causal determinants of design-induced error

When we look at a structure of human–system interaction, it can be assumed that the system can put operators into two states; cooperating or deteriorating state. A

cooperating state refers to a good state of operators to achieve a goal of tasks. In this state a system and operators in the system cooperate with each other. The system provides operators with relevant environments according to changing modes of tasks. It does not provoke or degrade human cognition. On the other hand, a deteriorating state means a state of design-induced error in which state the system has degraded the ability of the operator, leading to making errors.

How to differentiate one state from other, namely what are the determinants of design-induced error? In order to answer the question, in the thesis three causal factors of design-induced error are introduced: degree of complexity of a system; context of temporal decision-making condition; and existence of local rationality between designers and operators. Figure 4.10 depicts the way causal conditions in inherent system properties lead to design-induced error with a causal determinant.

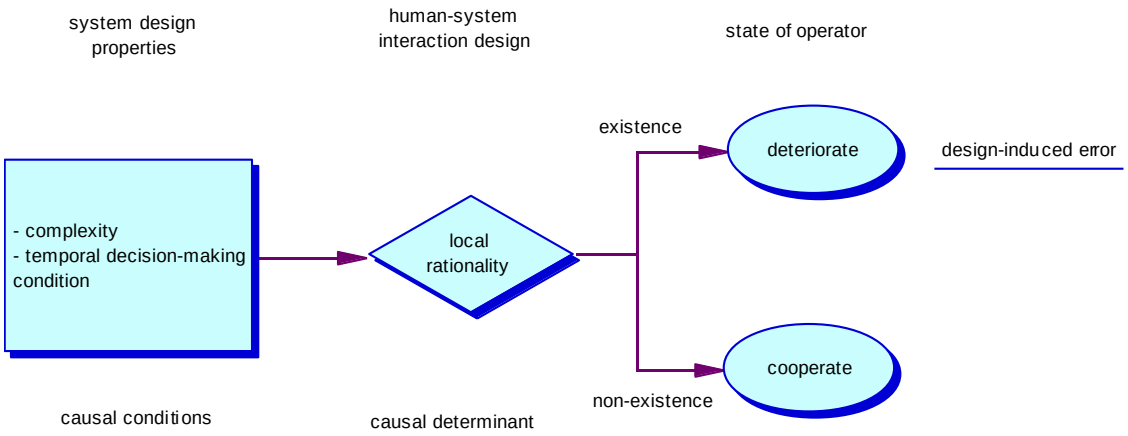


Figure 4.10 Development of design-induced error

Complexity and temporal decision-making error are conditions in which design-induced error can occur. From a contextual paradigm, a local rationality is regarded as a causal determinant of design-induced error because different perspectives on the system environments have led human operators to mis- (or non-)recognition and inappropriate performances to the system operation. Causal determinant is a generative mechanism of design-induced error.

Causal condition of design-induced error

- **Degree of complexity**: complexity of systems or tasks is not only a

necessity of modern systems but also a critical hindrance to human operators.

- **Context of temporal decision-making condition**: appropriately conducting tasks in a system depends on the context in which operators are situated to perform the tasks.

Causal determinant of design-induced error

- **Existence of local rationality**: how has a system been developed with different concepts from operators?

4.6.2 Interpretation of the meta-theory of design-induced error

From the meta-theoretical framework above, local rationalities between designers and users, the causal determinant of the meta-theory of design-induced error, have a power to interpret each phenomenon (Table 4.8). These differences are apparent in the goals, ability, and trust that each party attributes to the system. Every theory can be explained with the assumption. From the interpretational view of local rationalities between designers and operators, the meta-theory appears when designers design a system contrary to users' intention and ability. Table 4.9 shows the consequences of design-induced errors in each phenomenon.

The first theory, *risk homeostasis*, proposed by Wilde [1982], indicates that designers' attempts to reduce the risk of catastrophic failure through increased reliability or increasing number of hard defences, such as anti-lock braking systems on motor vehicles, may be defeated by user behaviour. The users of such systems may assume that the changes to the system allow them to safely increase productivity or performance. In this case, the user and the designer have different goals, the designers have a goal of reducing risk, but the users concentrate on another goal, that of increasing productivity.

The second theory, Bainbridge's theory of *ironies of automation* [1983], suggests that designers may believe that the reliability of the system can be improved by excluding the human from the operation of the system. However, as Bainbridge noted, it is impractical to remove the user from the system. This still appears a plausible proposition given that the human user possesses the unique ability to perform at the

knowledge-based level of performance, required to solve problems that arise in the operation of the system. Automation can gradually erode the ability of operators because they are deprived of experience in using the artefact. As a result, the eroded operator ability may reduce the operator's ability to diagnose faults and plan their use of the system.

The third theory, Muir and Moray's theory of *trust in automation* [1994], noted that that as a result of increasing computerisation of systems, the increasing complexity of systems, and the degraded ability of operators to deal with problems in the system, more and more users tend to place inappropriate trust in the system, and fail to check all relevant indicators. This may not match the expected degree of monitoring prescribed by the designers of the system.

The theory of Sarter at al. [1997] of *automation surprises* suggests that designers and users have different views of automation. The designer expects that the user constantly monitors the state of the automation and is able to respond to discrepancies in feedback that arise which illustrate that an error, arising from either the actions of the user or from a technical malfunction, has occurred. However, the users expect the system to serve them by providing readily-interpretable feedback about the state of the system

The theory of Hutchins, Hollan and Norman [1985] of *gulf of execution and evaluation* shows how designers and operators have different views on functions in a system. An artefact has functions with which operators can achieve a purpose or task. Problem solving is a main characteristic of human cognition. However, the cognitive ability of problem solving is limited and not always correlated to system functions. Designers expect that users will understand and serve the artefact to achieve its feedback and a goal, but users expect the artefact to serve users to achieve their goal by giving relevant and semantic feedback.

The remainder of the theories illustrate the manner in which the perception of the affordances of artefacts can lead to unanticipated usage. Busby and Hughes' theory of *plan delegation* suggested that designers expect that users are responsible and make plans, but users expect that artefacts exist to support the goals they wish to pursue.

Similarly, Norman's [1998] theory of *affordance* illustrates how the user expects that the properties of the artefact will suggest how to complete a task, whilst the designer assumes that these represent a means of accessing specific functions of the system. The features of an artefact provide different cues to designers and operators. Designers think that features represent a means to access functions, while users think that these features tell them what they must do.

THEORY	DESIGNERS' RATIONALITIES	USERS' RATIONALITIES
Ironies of automation	Introduction of increasingly reliable automation allows exclusion of unreliable user from the system	Systems are able to present information that is opaque and uninterpretable
Trust in automation	Users are able to generate an accurate mental model of the system and when monitoring should arise	Monitoring of the system can be based on own subjective perception of reliability
Automation surprises	Introduction of automation provides protection to the system	Introduction of automation should support reasoning about the state of the system
Design affordance	Affordances of artefact provide access to function	Affordances of artefact indicate the procedure required to complete specific tasks
Gulf of execution/ evaluation	Users serve artefact to achieve its feedback	Artefact serves users to achieve his/her goal
Risk homeostasis	Risk of failure decreased through use of increasingly reliable or defended systems	Increased reliability and defence can be exploited for increased performance
Plan delegation	Users are planful in their use of artefacts and will deploy in accordance with the goals prescribed by designers' recommended usage	Artefact can be relied upon to support acquisition of desired goals

Table 4.8 A contextual (local rationalities of designers and users) meta-theory of design-induced error

PHENOMENA	CONSEQUENCE OF DESIGN-INDUCED ERROR
Ironies of automation	If automation is introduced without considering the abilities of operators, the operator will lose their ability, especially in monitoring a state of system or diagnosis of a problem, to deal with problems.
Trust in automation	If a system needs a decision from human operators while conducting an automatic operation without continuous communication with the operator, the operator would rather rely on their own mind than reason about the situation.
Automation surprise	As a system activates a self-protection program without involving operators in the activity, the operator does a task expecting a different consequence, resulting in errors.
Design Affordance	As forms of signals, shapes, or locations of managing artefact is matched with natural human perception or physical performance even if an intention is different from the signals, users will act inadvertently against their will.
Gulf of execution/evaluation	If a system does not provide information in a form psychologically relevant to humans, users will be confused with the information while searching for a command or diagnosing a situation.
Risk homeostasis	If a system allows users to overestimate or be overconfident about the safety or reliability of the system, the user tends to exploit to the maximum the ability of the system.
Plan delegation	If a system delegates procedures that rely on human memory and does not prepare settings to notice the procedure, the operator assumes that the procedures are prepared by the system or forgets the procedure.

Table 4.9 Consequence of design-induced error

4.7 Summary

In this thesis, it has been argued that a meta-theory of design-induced error is necessary in order to provide a collective view of design-induced error. Consequently, it was necessary: (1) to elucidate the nature of design-induced error, and (2) to bind the scope of applicability of various perspectives on design-induced error. By revealing underlying structures of theories, and adopting the ontological assumptions and a contextual paradigm, a meta-theory of design-induced error has been developed. The main components of design-induced error are the following:

Three ontological layers of design-induced error: Affordance level; psychological logic level; and trust level.

A causal determinant of design-induced error: Existence of local rationalities of designers and operators.

Two causal conditions of design-induced error: Degree of complexity of system/tasks; and context of temporal decision making condition.

Three distinctive perspectives that categorise related theories on design-induced error have been presented. Each one of them refers only to certain aspects of design concepts in design-induced error. The affordance level of design perspective focuses on the observable practices of system and operators. It attempts to offer links between the various design features and their function.

The psychological logic level of perspective illustrates how psychological disconnection between logics and functions of a system can lead human operators to make errors. According to the psychological logic perspective, the function design in a system needs to be carried out in response to given logical requirements and the logic should be same in operators' psychological logic. Finally, the trust level perspective locates design in its wider socio-technical context. It is argued that currently our socio-technical systems need to be sure human operators in the system can develop a reasonable belief in a system, and this failure is the most important characteristic of design-induced error in socio-technical context.

All the preceding perspectives deal with different aspects of design-induced error in a manner that may appear too heterogeneous to synthesise. However, drawing on the ontological assumption, it has been suggested here that these perspectives can be conceived as dealing with three different, yet logically connected, ontological layers of

design-induced error. Different layers exhibit different connections between design elements (i.e. feature, function, logic, and reliability) depending on humans' recognition, understanding, and trust in the elements. Each layer constitutes a relatively autonomous area of study, and the transition from each layer to the one below it denotes an interest in penetrating deeper into the object of study and investigating the conditions that render the preceding layer possible.

The rationale behind the conceptualisation of design-induced error was described with a concept of causal factors of design-induced error that are derived from the roles of a system and a human operator in a human–system interaction structure. From a contextual paradigm, we can assume that different perspectives on the system between designers and operators can determine the design-induced error. The causal conditions that create adverse environments for operators are external contexts of a system. On the other hand, the causal determinant, a local rationality between designers and operators, is an internal factor and not shown as a physical context. It appears in human–system interaction failures. The degree of causal conditions of design-induced error is dependent on the existence of causal determinant.

This meta-theoretical conceptualisation of design-induced error presents four advantages. First, it provides a collective view of related theories that show design issues in human–system interaction failures. Against a current situation in which we identify only each theory separately, a meta-theory that has ontological layers in which we can make connections between layers provides us with a whole view of design-induced error.

Secondly, the various perspectives on design-induced error have been logically related to each other in terms of design-induced error. These logical relationships elucidate that in order to construct a cooperating system each design element should be integrated consistently with human cognition and performance. The existence of particular features of design-induced error at a particular layer is only a necessary (but not sufficient) condition for the existence of features at the preceding layer. The important characteristics of design reveal that designers have to consider what design can do, and what design means to the operator.

Thirdly, the meta-theoretical assumptions proposed move beyond an equipment design perspective. Including a socio-technical design point of view is possible. In an equipment design, level of design-induced error confines itself to the observable design-induced error practices only. This level is unable to offer explanations of the possibility of a relationship between high levels of design elements (i.e. logic, and reliability of a system). It may difficult to describe, for the equipment design

perspective point of view, outlining what design is capable of doing.

Finally, with an assumption of causal determinant of design-induced error (local rationalities between designers and operators), an analytical and explanatory tool for what and how a human–system interaction failure is caused has been developed. The meta-theory of design-induced error is an interpretational methodology for analysis of human–system interaction failures in terms of a role of design. With the methodology, any readers who want to understand human–system interaction failures can develop a proper reasoning about the failure to find design issues that would easily have been missed or underestimated without such a methodology. This meta-theory may be used in a design process as well as in accident analysis. The meta-theory will be also examined for analysing a specific accident report system in terms of the role of design. The result is reported and discussed in chapter 5 and 8.

There were limitations in this thesis while developing the meta-theory. Firstly, this thesis did not create a new theory. It is rather a contextual and ontological combination and interpretation of related theories. This approach produced a collective understanding of related theories in the light of a relation between design purpose (i.e. perspective of designer) and human error (perspective of operator). The meta-theory developed in this thesis is not only one meta-theory of design-induced error. Other people can make other meta-theories with their own assumptions and paradigms.

Additionally, the number of theories that appear in the meta-theory of design-induced error is not exhausted. There may be other theories that explain the problem above. This research, however, used the theories above only because it is not a main focus of this research to search how many theories exist but how to provide a collective view of related theories. Other researchers can include other theories if necessary.

A definition of Design-induced Error: In its broadest sense, design-induced error can refer to any error made by a user of operator of an artefact or system which is partly or wholly attributable to the design of the artefact or system. In this dissertation this definition is acknowledged, but a narrower view is taken, based on local rationalities between designer and user. In this regard, there are two key aspects of any good definition of design-induced, the first of which is a definition of what errors are design-induced and what are not, and the second is a definition of the limitations that go with "design-induced". This means, how to differentiate other human errors from design-induced error.

In the proposed meta-theory, design-induced may be judged as a function of different perspectives between designers and operators. If an error originates from a difference in expectation and intention between designers and operators, it can be considered as

having a characteristic of a concept of design-induced error, otherwise not. For example, if a pilot made an error by misinterpreting a signal in a cockpit display and the misinterpretation was not caused by any malfunction of the pilot's physical health but due to the human reasoning process of normal pilots, this error can be categorized as a design-induced error, because there was a different perspective between designers of the system and the pilot. The designers had an expectation that pilots in the system would clearly recognise the signal in the display and perform correctly, but the pilot had a different expectation of how the design of the cockpit display could provide a reasonable feedback (e.g. if the pilot selects a wrong number, then the system alerts the pilot in an appropriate manner).

On the other hand, if a system fails to transfer an intention of designers in a function to operators, it should be classified as a "design (engineering) failure", because this error was not caused by different perspectives between designers and operators. The intention of designers was not communicated to operators due to a system failure. For example, an operator made an error based on wrong information provided by a system. A malfunction in the system created the wrong information. In the case of this error, we cannot say the operator error was a design-induced error because the system failure was not the intention of the designers as part of the design.

However, it is possible that an error can be classified as design-induced error if the designer designed the system with an intention that there would be an error in the system, and that the operator could cope with the error. On the other hand, the operator conceived that the designer prepared for the system error. In this case there was different perspective between designers and operators.

As an error was not related to the intention of designers, the error may be not classified as a design-induced error. This case does not conceive different perspectives between designers and operators. For instance, an operator misread a direction in a gauge due to fatigue of the operator and the fatigue was not created or increased by tasks related to the system. This should be classified as a "personal oriented error".

In summary, design-induced error is defined here as error made by a user of operator of an artefact or system which is partly or wholly attributable to differences in the rationalities of the user and designer of the artefact or system.

Chapter 5. Case Study: Results of the meta-theory application to accident cases

The previous chapter presented a meta-theory of design-induced error. This chapter presents case study results of accident analysis with the concept of Design-induced error meta-theory. The case study was conducted in order to answer the following questions:

- What is nature of human errors in real accidents?
- How to capture the concept of design-induced error in the accident cases? How can the meta-theory of design-induced error help to identify design issues in human errors (mechanisms of errors and implicated design concepts that affect human operators)?
- In which ways can people be helped to understand design issues in human error? Is there any way to represent relationships between design and human error?

The case study used the same accident data-set taken from the Australian aviation accident report database system that was used during developing the ontology. The first section 5.1 of this chapter discusses the overall results of the analysis by summarising the quantitative results. Section 5.2 clarifies and examines artefacts or systems that fail in the course of human–system interaction. Section 5.3 presents diagram analyses in which relationships between human errors and systems may be more easily represented. The final section 5.4 presents the summary and limitations of this study.

5.1 The overall results of the case study

Nature of Accident involved in human–system interaction failures

This section shows the quantitative results of this case study. 562 accident cases were examined and categorised. The analysed results were reviewed by a human error specialist. However, it is important to mention that the results are not strictly statistical and the data or findings in the accident reports were accepted as truth. The aim of the study is to see a general tendency of human errors in accidents rather than statistical exactitude.

The first research question is:

What is the nature of human error in real accidents?

The question may have the following sub-questions:

- How many human error cases could be found in accident reports?
- In which artefacts or systems do human operators make errors frequently?
- When do such failures occur?
- What kinds of jobs/tasks are involved in the errors?

The remaining parts of this section present results of accident analysis.

The portion of human error cases in accidents

In order to answer the first sub-question about the portions of human error in accidents, the accident data set analysed the categorised accident types. The classification of general accident types are; mechanical failure, operator failure, external factors, or unknown.

- Mechanical failure: an accident mainly caused by mechanical failure (e.g. failure of a motor).
- Operator failure: an accident caused by human error (e.g. wrong management of a device).
- External factors: an accident caused by external factors such as bad weather.
- Unknown: the causation of an accident could not be identified by investigation.

Table 5.1 Accident type

ACCIDENT TYPE	NUMBER OF CASES	PERCENTAGE
Mechanical failure	204	33.01%
Operator failure	287	46.44%
External factor	56	9.06%
Unknown	71	11.49%
TOTAL	**618**	**100%**

By analysing accident reports, the study found that 287 cases fall into the human error category (operator failure). This is 47% of all accidents examined. If more than one accident causation was found, all factors were counted at the same time. For example, if there was a failure of a part of a mechanical system and then operators' failure was also found, that case was recorded the case in the category of operator failure as well as the mechanical failure category. Table 5.1 shows the portions of accident types in the dataset.

Human error types

Human error types are further categorised into 14 items in reference to commonly used human error terms in many research studies. The "not recognising" error is the top cause of errors, "misinterpretation", "misunderstand", and "inappropriate performance" follow. Table 5.2 shows the result.

Table 5.2 Human error type

HUMAN ERROR TYPE	NUMBER OF CASES	PERCENTAGE
Misreading	19	5.29%
Miswriting	8	2.23%
Misinterpretation	51	14.21%
Misunderstanding	50	13.93%
Did not recognize	75	20.89%
Inattentional activity/ automation mode	13	3.62%
Inappropriate performance	50	13.93%
Not following the signs or indications	5	1.39%
Not keeping monitoring	19	5.29%
Violation of rules or procedure (if there is other benefit for the task or whole system)	21	5.85%
Not doing	6	1.67%
Not checking	31	8.64%
Difficult to understand	7	1.95%
Forgot to do	4	1.11%
TOTAL	**359**	**100.00%**

Factors leading to errors

Operators are often confused with similar conditions and procedures. Design of operation and function provided by a system need to be designed more carefully in order to misidentify.

What kind of information systems give operators is an important factor that leads to errors. If a system does not give information, operators have to make assumptions about the situation. That leads to errors. **Table 5.3** shows the result.

Table 5.3 Factors leading to human error

FACTORS LEADING TO HUMAN ERROR	NUMBER OF CASES	PERCENTAGE
Providing different possibility	37	10.54%
Hiding important property	53	15.10%
Confusing with amount of information	47	13.39%
Confusing without information	18	5.13%
Providing unreliable information	9	2.56%
Conflict with previous experience etc.	26	7.41%
Difficult to deal with the artefact	45	12.82%
Not providing relevant information	7	1.99%
Too much reliance on the system	28	7.98%
Difficult to distinguish	55	15.67%
Providing a method unfriendly and less used before	4	1.14%
Making it easy to do or access a wrong way of using the artifact	22	6.27%
TOTAL	**351**	**100.00%**

Meta-theory classification

In the previous chapter, human errors were analysed in terms of meta-theory classification. The gulf of evaluation is the most commonly found among the theories in the meta-theory. It means that many of operators involved in failures failed to evaluate a current situation or state of a system. Cases of automation trust were found as well. The aviation industry has adopted sophisticated artefacts and systems resulting in complexity and automation. There have been tendency of operators relying on those artifacts or systems. Table 5.4 presents the result. In this classification the theory 'automation ironies' has two sub categories; inability(degraded abilities of operator dealing with problems in an automation system) and monitoring failure because the theory explains the two phenomena.

Table 5.4 Meta-theory classification of design-induced error

THEORIES IN META-THEORY OF DESIGN-INDUCED ERROR	NUMBER OF CASES	PERCENTAGE
Automation ironies (inability)	44	10.76%
Automation ironies (monitoring failure)	26	6.36%
Trust in automation	57	13.94%
Automation surprise	12	2.93%
Design affordance	39	9.54%
Gulf of execution	42	10.27%
Gulf of evaluation	104	25.43%
Risk homeostasis	33	8.07%
Plan delegation	52	12.71%
TOTAL	**409**	**100.00%**

5.2 Analysis of failed artefacts or systems

The Australian aviation accident reports system (AAARS) database for the period from 1994 to February 2005 has been examined, and a dataset provided in the Microsoft Excel and Access database for 223 human-error cases. As some occurrences involved other accident types, the original dataset of operator errors was higher (n=287) than the number in the dataset for the analysis. . A complete list of the dataset is presented in Appendix B.

5.2.1 Overview of failed systems

The failed systems in human–system interaction failures were grouped into ten themes that were identified in the course of accident analysis. Among those cases some informative cases were examined in detail. Table 5.5 shows the result.

Table 5.5 Items of failed systems during human–system interactions

	FAILED SYSTEMS	TOTAL
1	Air traffic control system (TAAATS[12], ASD)	**10**
2	Cockpit control system (FMS, FMC, CATIS, chart)	**14**
3	Handles or switches (Landing gear/flap, switches)	**12**
4	Fuel selection/ fuel management system	**24**
5	Warning systems (TCAC, stall warning, weather radar, GPS)	**20**
6	Monitoring system	**14**
7	Traffic communication system (CPDLC, radio etc.)	**92**
8	Procedure/emergency procedure system	**16**
9	Wire (power line) detecting system	**12**
10	Runway safety system	**9**
	TOTAL	**223**

[12] TAAATS: The Advanced Australian Air Traffic System

The following sections present analysis results according to system themes with 55 examples. In the example, dotted lines and background shades provided would help to identify human error and system functions that led to human errors. Table 5.6 presents mark-up index.

Table 5.6 Mark-up indices for identifying design-induced error terms

MARK-UP INDEX	EXPLANATION
Human error	Human errors
Design deficiency	Design deficiencies associated with human errors
Modification of design	Modification of design after the failure

5.2.1.1 The air traffic control system

Air traffic control systems are important for organising aircraft on departure, arrival or en route in order to prevent air traffic congestion or even collision that can result in tragic accidents. Many sophisticated artificial systems have been developed in order to provide air traffic controllers and pilots with situation awareness.

The Australian Advanced Air Traffic System (TAAATS)

Functions

TAAATS (pronounced tats) is the hardware and software system used by Airservices Australia for Air Traffic Control services. It is a computer based system, which serves as an aid to Air Traffic Controllers. It does not control aircraft, but gives the user a display of information about an aircraft's position and associated information. It also handles communications and other information exchanges [From Wikipedia, November 2007, available in http://en.wikipedia.org/wiki/The_Australian_Advanced_Air_Traffic_System].

TAAATS is a sophisticated integrated air traffic control system that provides accurate and enhanced information on aircraft movements. TAAATS control station has four computer screens:

Air Situation Display (ASD) : This main screen is basically a map of the sector that shows the location of all aircraft in controlled airspace, as reported by one of several data sources – radar data processing, flight data processing and automatic dependent

surveillance.

Miscellaneous Information Display : A display providing access to a wide range of information including aircraft performance data, weather radar, airport/navigation aid/tracking point codes, airline ICAO designators, Standard Arival Route (STAR) and Standard Instrument Departure (SID) "plates" and depiction of the airspace setup for TMA sectors.

Voice Switching and Communications Select (VSCS) panel : A touch-sensitive screen allows controllers to choose the radio frequency they need to talk to pilots and ground staff, or the intercom for talking with other controllers.

Auxiliary Display : The controller can call up a wide range of information such as weather forecasts, flight plans, strip windows, secondary maps and other material for the information of themselves and pilots.

Error modes

When there are many things to do simultaneously or in an automatic process, operators of TAAATS may fail to conduct careful selection of each function displayed in computerised systems because most selections can be achieved by just entering a key on a keyboard (example 1, example 2). It is an easy task to type in a keystroke, resulting in unconscious performances. For instance, in example 1 there were many deleting functions in the computerised monitor. The coordinator in example 2 suffered from reviewing flight progress strip. With combination of circumstances, if there is not a clear preventive function provided by the system, it may lead to operators' unintentionally entering or deleting data. The configuration of the system may make it easy for operators to make errors.

Example 1

> the Cairns Tower coordinator controller had cancelled the aircraft's flight data record in The Australian Advanced Air Traffic Control System (TAAATS). … The coordinator had assumed that an aircraft on the ground at Cairns was the aircraft displayed as airborne and consequently felt that it was unnecessary to check further prior to deleting the record. TAAATS displays a warning message requesting confirmation of the cancellation action when a controller deletes a flight data record for an aircraft. This message does not warn controllers that they do not have jurisdiction of the aircraft. … Airservices Australia have proposed that the warning message

> for non-jurisdiction flight data records should be amended to alert controllers to the fact that coordination is required prior to deleting the record. (This is one of many TAAATS software modification requests that have been submitted.) *ATSB occurrence No:199805341*

Example 2

> the Adelaide strip for HYY was accidentally placed on the airways clearance delivery console and the Sydney strip placed on the surface movement control console. … The coordinator did not review the flight progress strip to ensure the crew had been cleared before coordinating the Sydney flight data record for VH-HYY…. Local safety action: Airservices Australia Southern District issued a request to amend the TAAATS software to: Show when there is more than one record in the system for an aircraft during the preactive stage. Amend procedures so a clearance is annotated on a flight progress strip only after it is issued. *ATSB occurrence No:199905168*

Air Situation Display (ASD)

Functions

The air traffic control air situation display provides controllers with an automatically triggered alert when a variation is detected, by radar, between the planned track and the actual track being flown.

Error modes

When there is data that represent a position or condition of a system, operators consider the data displayed as an actual state of the system even the data was input before. If there is no correction and checking system, incorrect data input that should have been checked could misguide operators to believe the incorrect input data as showing a real position through ASD (example 3). In a complex display (Figure 5.1) it is difficult for human operators to identify the correct position and procedural tracks of all aircrafts. It might not effectively warn operators if there were warning signals illuminating routinely. Combined with an ineffective alert system the ASD system may confuse the operator causing failure to recognise situations before encountering a serious condition

(example 4, 5).

Example 3

> The position of the Boeing 767 was displayed incorrectly on the Brisbane sector controller's Air Situation Display (ASD). The aircraft passed ATMAP at 0404 Coordinated Universal Time and was estimating Curtin at 0503. At 0404 the aircraft was displayed on the ASD just south of Bali with an estimate for Bali of 0404. Bali ATC had previously advised Brisbane ATC that the aircraft was estimating ATMAP at 0404. As the aircraft was not within radar coverage and not fitted with Automatic Dependant Surveillance equipment, the ASD displayed the aircraft position consistent with the input data, not the aircraft's actual position. … The investigation revealed that the controller had used the electronic strip intending to enter the time of 0404 for ATMAP, but instead entered 0404 as the time overhead Bali. *ATSB occurrence No:* 200000933

Example 4

> The controller had not established that the two aircraft had definitely passed, or that a longitudinal separation standard existed in accordance with the MATS, and vertical separation reduced to less than the minimum 1000 ft standard. The routine display of CLAM alerts for expected events, such as the issue of discretionary climb, did little to enhance the controller's situational awareness in regard to QF31s cleared level status. … In addition, The TAAATS Alerts Review and Enhancement Project is currently reviewing the processing and display of CLAM and other alerts for controllers. Software is currently being developed to allow a flight plan conflict function display for procedural tracks, including ADS tracks, for delivery late in 2006. *ATSB occurrence No:* 200404707

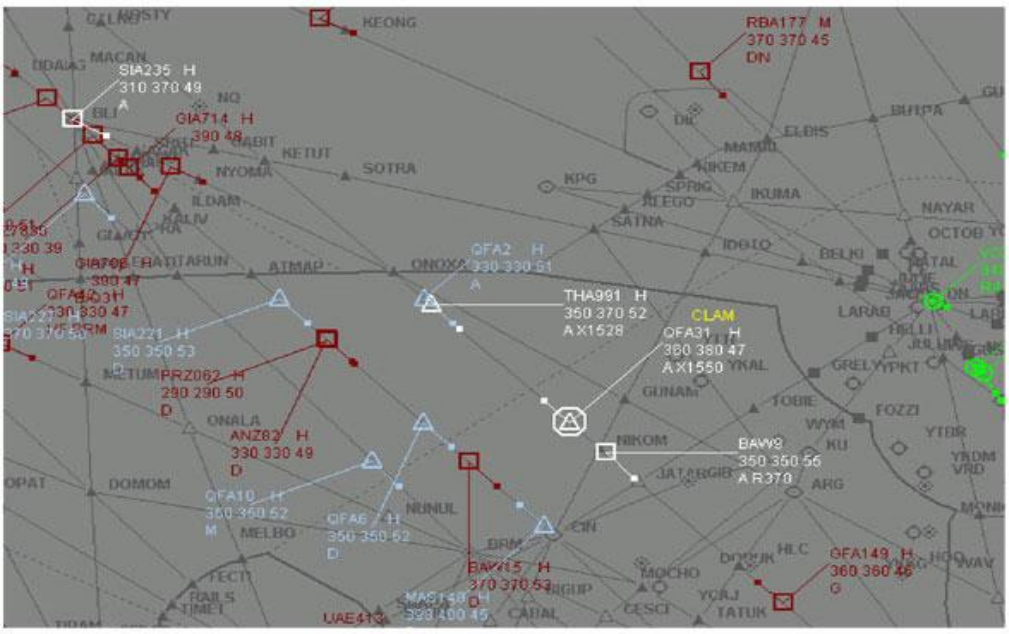


Figure 5.1 Airservices Australia computer replay at 1524UTC[13] (in example 4)

Example 5

> The air traffic controller's initial scan of the air situation display was incomplete and did not detect that a procedural separation standard would not exist between the 737 and the 777, or that he needed to calculate the time that the 10 minute longitudinal separation standard was established. … A more comprehensive initial scan of the air situation display by the controller may have facilitated timely action to avoid an infringement of separation standards. *ATSB occurrence No:* 200600396

Computerised automatic terminal information system (CATIS)

Functions

[13] The replay was created from recorded data, used for investigation purposes, by Airservices Australia. It was not taken directly from the air situation display (ASD) that the controller was viewing, and does not necessarily reflect all the information, or the display setup, presented to the controller at the time of the incident. Airline flight number QF31 is displayed on the ASD as QFA31 and TG991 is displayed as THA991.

The computerised automatic terminal information system (CATIS) is used to broadcast operational information to pilots. The CATIS was normally broadcast on the non-directional navigation beacon (NDB) and a very high frequency (VHF) radio transmitter.

Error modes

In the example 6, operators have trusted information provided by the CATIS and not checked further. However, limitations of the system meant that it could not include all the information that should be available.

Example 6

> The controllers in the Adelaide Air Traffic Control tower had previously included information that the LLZ[14] and the GP[15] were not available on the computerised automatic terminal information system (CATIS) that is used to broadcast operational information to pilots. When the LLZ was returned for operational use, they abbreviated the advice to `localiser available', due to system constraints on the amount of additional information that could be included. The information that the GP was not available was not included in the CATIS. *ATSB occurrence No:* 200400856

The console of the air traffic control system

Error modes

Insufficient operating positions (limited space in example 7 and 8, position of the controller pilot datalink and the sector 8 operating console in example 9) increase possibilities of errors by controllers. Especially, in very busy times, operators are easily distracted, resulting in them making errors or missing information.

Example 7

> KAL362 was incorrectly given a clearance to climb to FL290

[14] LLZ: Localizer

[15] GP: Glide Path

> by the Bangkok Sector 3 controller, … A high level of interaction and cooperation was required between the radar and procedural controllers to effectively manage the sector's airspace. The flight progress strips for each aircraft were required to be retained in the procedural display until the crew reported at the next position. This was to enable controllers to observe that an aircraft was in transit between the previous and next positions. However, due to limited space to display the strips, the Sector controllers had developed a habit of removing flight progress strips at the earliest opportunity to make space for new strips. *ATSB occurrence No:* 199702691

Example 8

> Both controllers had earlier noted the possibility for conflict between the two aircraft and annotated their respective flight progress strips with an Oodnadatta position, and the calculated estimates for that position. … During the following 90 minutes, the traffic level steadily increased …He was unable to monitor the Sector 1 controller's air-ground-air program on a continuous basis due to the conduct of coordination actions. The work at the console was difficult, with three controllers working in an area normally used by only two controllers. *ATSB occurrence No:* 199804690

Example 9

> The distraction and subsequent failure of the sector controller to regularly scan the flight progress strips. … The positioning of the controller pilot datalink and the sector 8 operating console restrict the ability of controllers to maintain an effective scan of the flight progress strip board. Controllers are required to divert their gaze and attention from the board to operate the controller pilot datalink keyboard. Modification of the console layout to enable more ready access to the controller pilot datalink or alternatively, provision of a controller to operate the controller pilot datalink during busy traffic periods would alleviate the problem. *ATSB occurrence No:199802755*

The surveillance radar (SURAD)

Functions

The surveillance radar (SURAD) equipment is designed to help the air traffic controller to identify the tracks of aircraft.

Error modes

In case of example 10 where errors were associated with SURAD, the SURAD did not have identification labels or height information (facilities that were available on more modern equipment) and that limitation increased the workload on the controller.

Example 10

> The controller had omitted to issue the 7,000 ft restriction even though it was still a requirement to ensure separation with inbound aircraft. … Additionally, the SURAD was unreliable in its ability to provide constant, accurate position information within 10 NM of Williamtown. The controllers were aware of those restrictions as they were documented in aeronautical publications. The military sector controller was using the Interim Radar Display System (IRDS). Although that system had labels and a Mode "C" height reading capability, the Macchi was not equipped with a Mode "C" capability. Consequently, the sector controller did not have a radar indication of the height of the Macchi. … flight progress strip management made the task of remembering an additional restriction more complicated. Consequently, the trainee approach controller forgot to issue the 7,000ft requirement to the crew of the Macchi. *ATSB occurrence No:* 200004806

5.2.1.2 The cockpit computer system

In order to help pilots to identify situations, computerised cockpit systems have been developed such as the flight management system, flight management computer etc. These systems fitted to the aircraft provide various functions such as lateral and vertical flight path guidance as well as performance information to the crew. The systems can also provide control and guidance information to the autopilot. Most systems are displayed on the monitor fitted in the cockpit.

Flight Management Computer (FMC)

Functions

A Flight Management Computer is a computer carried on an aircraft to integrate the functions of navigation and performance management. It is composed of two kinds of database: Navigation and Performance of a certain aircraft. The FMC is the heart of the modern aeroplane's electronic systems, and gathers information from other subsystems (Wikipedia, http://en.wikipedia.org/wiki/Flight_Management_Computer).

Error modes

Before the FMC can be utilised to provide vertical navigation guidance, it needs to compute a descent path, which conforms to the requirements of the instrument approach. Waypoints and associated altitude constraints required by the FMC to compute an accurate approach profile that correspond to the LOC/DME approach path gradient should be input by the crew. It is necessary to input data (e.g. altitude constraints) into the FMS in order to intercept waypoints. However, the screen can be changed into other modes without notice during the work. **Figure 5.2** shows the display of example 11 cases before entering data and the display change into other mode automatically in **Figure 5.3**. When the system did not provide protective measurements against the crews' inadvertent performances, the crew omitted waypoint/altitude constraint data from the flight management computer (FMC) LEGS page (examples 11, 12), or mistakenly entered data in the active flight plan page on the multi-function control and display unit of the flight management system (FMS). The columns moved automatically without the operators noticing (example 13).

Example 11

> The flight crew misinterpreted the holding pattern limit from the runway 35 ILS approach chart. … The flight crew did not monitor the Canberra DME to check distance on the holding pattern outbound leg until they had proceeded beyond the holding pattern limit. Significant factors 1. The MEL applied to the aircraft allowed continued operation when elevated temperatures caused the environmental conditions on the flight deck to become abnormally hot, contributing to pilot fatigue during a long flight sector. 2. The assistance of air

traffic control radar services, which is normally provided, was not available to the crew. 3. The holding pattern limits published for CCK, did not contain the referenced DME identifier (Canberra) in the limit notes. 4. The copilot, under the direction of the pilot in command, entered incorrect data in the FMC. 5. The pilot in command did not detect the incorrect entry in the FMC. 6. The flight crew did not employ effective means to verify the navigational performance of the FMC. *ATSB occurrence No:* 200402747

Figure 5.2 FMC CDU display showing hold page before the leg distance had been entered.

Figure 5.3 FMC CDU display showing hold page after the leg distance had been entered.

Example 12

> The crew selected the appropriate approach and landing charts and programmed the flight management computer (FMC) for an arrival to runway 15. Three minutes before the crew commenced descent, the ATIS was changed to indicate that arriving aircraft from the south could expect to carry out the runway 33 Locator/Distance Measuring Equipment (LOC/DME) approach to runway 33. The crew was not aware of the change … During that interaction the crew did not select waypoint HENDO as the IAF when prompted by the FMC to do so and consequently critical 'Not below 6,500 ft' altitude constraints at the HENDO and 20 DME Cairns waypoints were omitted. *ATSB occurrence No:* 200401904

Example 13

> In order to ascertain the predicted altitude that the aircraft would overfly Mackay, the crew removed the constraint

> altitude relating to the overhead Mackay position. It is likely that, when the crew reinstated the overhead Mackay altitude constraint, the altitude constraints for subsequent flight plan segments were applied to the immediately preceding segment. A break (or discontinuity) in the predicted track on the map display screen (a normal feature in the operation of the system) distracted the crew during the inbound turn, during which time the aircraft descended below the step altitude (2,200 ft). … The sequence of FMS entries advised by the aircraft manufacturer provided an explanation of how the 2,500 ft step altitude, once removed, could have been incorrectly reinstated into the active flight plan. This meant that the FMS contained an incorrect step altitude for the inbound turn and that the automatic flight system would allow the aircraft to descend below the step altitude unless the crew intervened. The crew believed that they had operated the FMS system appropriately and were unaware that the constraint altitude had been changed. It is likely that they expected that the aircraft's automatic flight system would not infringe the vertical profile limits of the approach. However, it was apparent that they became distracted during the inbound turn by the track break or discontinuity on the map display. *ATSB occurrence No:*200302433

Chart in the cockpit computer system

Error modes

Design tries to put more information in a single form of data display. As a result the depiction on the form may be complicated and small, which sometimes make it difficult for people to identify a position wanted from other positions. If depiction in a chart is difficult to identify, it may impair identifying positions in the chart in example 14. Example 15 illustrates confusion of same letters displayed in a chart.

Example 14

> The crew of a Boeing 767 (B767) had been cleared to taxi for departure from runway 01, intersection "A7", at Brisbane. They proceeded along taxiway "B" then, incorrectly, initiated a turn onto taxiways "B5" and "A", which was in conflict with rapid

> exit taxiway "A5S". A BAe146 vacating runway 01 via "A5S", was instructed by ATC to hold short of taxiway "A" in order to avoid the B767. … The operator of the B767 advised that they had tried a new system of printing aerodrome charts from a computer application compact disk. However, the print format was such that the pilot in command of the B767 was not able to correctly read the notes provided on the chart with respect to taxiway routes and directions. *ATSB occurrence No:* 200105351

Example 15

> After a Boeing 747 had landed on runway 34L the crew was instructed to taxi via runway 25 and taxiway Yankee (Y). Jeppesen Sydney terminal chart 10-9, dated 18 December 1998, was used to provide taxi guidance to the crew. That chart depicted taxiways G3 and Y leading off to the north of runway 25. However, the chart was ambiguous in that there was another letter "Y" displayed to the south of runway 25. The crew interpreted taxiway G3 to be taxiway Y on the basis of that information. The crew subsequently turned the aircraft onto taxiway G3, which was closed. The aircraft was then stopped until cone markers and unserviceability lights, which marked taxiway G3, had been removed. … Jeppesen were advised of the ambiguity displayed on the chart and have since re-issued the chart to more accurately reflect the current amendments to the taxiway system in that part of the airport. … *ATSB occurrence No:*199900153

QNH barometric altimeter

Function

QNH[16] is a Q code. It is a pressure setting used by pilots, air traffic control (ATC) and low frequency weather beacons to refer to the barometric altimeter setting which will cause the altimeter to read altitude above mean sea level within a certain defined region. This region may be fairly widespread, or apply only to the airfield for which the QNH

[16] QNH: Atmospheric Pressure (Q) at sea level – i.e. the altimeter setting that allows the altimeter to read altitude about mean sea level

was given. An airfield QNH will cause the altimeter to read field elevation on landing irrespective of the temperature. ((Wikipedia, http://en.wikipedia.org/wiki/QNH , November 2007)

QNH is the mean sea level pressure derived from the barometric pressure at the station location. The local QNH at an airport is normally derived from an actual pressure reading. Australian aviation regulations require that, when an accurate QNH is set on the pressure-setting subscale of an altimeter planned for use under the Instrument Flight Rules, the altimeter(s) should read the nominated elevation to within 60 ft. QNH should be set on the altimeter pressure-setting subscale of all aircraft cruising in the altimeter setting region, which extends from the earth's surface to the transition altitude of 10,000 ft in Australia. QNE[17] is the standard pressure altimeter setting of 1013.2 hPa that is set for flight above the transition altitude.

Error modes

Normally as it is not necessary to adjust barometric pressure in QNH, the pilot does not concern about resetting the barometer. In this case studied, the operator forgot to reset the barometer of QNH. There was no warning system at this case (example 16).

Example 16

> As the aircraft approached 500 ft above ground level, the rate of descent was assessed as too high … during this check that the pilots realised that the barometric settings on the altimeters had not been set to the airfield QNH of 1028 hectopascals (hPa) but rather had been left on 1013 hPa; the setting required for flight above the transition altitude (10,000 ft.) *ATSB occurrence No:* 200301990

5.2.1.3 Handles or switches

Pilots and air traffic controllers use operating devices such as handles or switches. Users have to remember how to use such operating devices and perform correctly in order to achieve the system's goals.

Landing gear/flap

Error modes

[17] QNE: 1013.25 Mb Altimeter Subscale Setting (International Standard Atmosphere)

There were four cases of wrong landing gear selection incidents. In most cases, the pilots involved in the accident unintentionally moved the flap/slats near the landing gear handle instead of the landing gear. They do not know the reason why they failed to perform the operation correctly. The position of artifacts and skill-based performances may be associated with the errors. In example 17, 18 show that pilots moved the flaps/slate instead of the landing gear.

Example 17

> Following a normal take-off the pilot in command (PIC), the handling pilot, called for the landing gear to be retracted. A short time later, he noticed an amber warning appear on the airspeed scale on his primary flight display (PFD) screen. … he noticed that the flaps/slats lever was at the `slats retract' position. … Interviews with the PIC and copilot did not reveal any obvious issue that might have led to the copilot retracting the flaps/slats instead of the landing gear. *ATSB occurrence No:* 200302037

Example 18

> After TJC became airborne the co-pilot, observing indications of a positive rate of climb, called for "gear up". The pilot in command reported that on hearing the "gear up" call, he observed his airspeed indicator to be at the speed when flaps would normally be retracted from the FLAPS 5 position to the FLAPS 1 position. Noting this airspeed, he positioned the flap lever to the FLAPS 1 position instead of positioning the landing gear lever to the UP position. However, he did not call "flaps 1 set" when the flaps reached the FLAPS 1 position, which should have been done in accordance with the operator's standard operating procedures. … The co-pilot was concentrating on maintaining the aircraft's flightpath and did not notice that the pilot in command had retracted the flaps instead of the landing gear. … As a result, on hearing the call for "gear up", and on noting that the airspeed was in excess of the initial flap retraction speed, he inadvertently substituted flap for gear and consequently retracted flap instead of the landing gear. *ATSB occurrence No:* 199903131

Bleed air switches

Error modes

In the cases studied in which performance of bleed-air switches was a factor, pilots failed to perform correct movements of intended switches. The pilot in the example 19 moved other switches near to the target switch (see Figure 5.4). The bleed-air valve switch was moved instead of vent fan switches. Example 20 also shows same pattern of an inadvertent move in a hectic situation (e.g. becoming occupied with reprogramming the aircraft's GPS setting.

Example 19

> The switches were placarded bleed-air valve (left and right), and the individual switch positions were (as read from the top selection to the bottom) OPEN, ENVIR OFF, and INSTR & ENVIR OFF. … The cabin pressurisation instruments were positioned low on the centre instrument panel, and were partially obscured by the engine and propeller control levers in flight. … The aircraft also had two vent blowers that forced air through underfloor ducts to assist with cabin ventilation. The vent fans were switched on when the aircraft was on the ground to prevent the ducts from overheating. As the aircraft climbed through 10,000ft the aft blower was normally switched off, and the vent blower was normally switched from HI to LOW. The vent fan switches were positioned directly above and below the right bleed air switch on the co-pilot's environmental sub-panel. The switches were of a similar shape to most other toggle switches on the instrument panel, and did not require pulling out of a detent before changing position. The switches were smaller and dissimilar in shape to the nearby bleed air switches. … Both bleed air switches were inadvertently selected to ENVIR OFF at about 10,000 ft in the climb. *ATSB occurrence No:* 199902928

Figure 5.4 Beech 200 cockpit layout, and an expanded view of the environmental sub-panel in example 19

Example 20

> Following take-off, at about 2,000 ft, the air traffic controller instructed the pilot to intercept the 173 radial at 120 NM from Tindal, and then to track along that radial to Tindal. That had been necessary to avoid the now active Military restricted area R248(B). The pilot reported that he had then become occupied with re-programming the aircraft's Global Positioning System (GPS). During the climb to the cleared level, Flight Level 130, the pilot reported that he believed that he had actioned all the required checklist items. … Once established at 10,000 ft, the pilot discovered that both the left and right bleed air OFF green advisory annunciators were illuminated, and that both bleed air switches were in the ENVIR OFF position. In that position, no bleed air was available for aircraft pressurisation. The pilot had then selected both bleed air switches to OPEN, and restored normal pressurisation. *ATSB occurrence No:* 200105188

Landing gear inhibit switch

Functions

The two-position (NORMAL and INHIBIT) landing gear inhibit switch is normally guarded (by a plastic cover to confirm position) to the NORMAL (OFF) position. The INHIBIT position provides an open electrical circuit to the landing gear-down solenoid of the gear selector valve, preventing normal operation of the gear and also preventing illumination of the LDG GEAR INOP caution advisory light. Selecting the landing gear inhibit switch to the INHIBIT position idled the normal landing gear extension system actuators to ensure unhindered operation during alternate extension. Alternate extension of the landing gear uses the freefall characteristics of the landing gear, and is used for emergency extension of the gear. The landing gear inhibit switch is also selected in flight crew training to provide the crew with realistic practice in using the alternate landing gear extension system.

Error modes

A normal setting (e.g. positioning of switches) can be changed by unexpected results (such as maintenance work as in example 21). If there are no proactive procedures or alert systems, the human operators may assume the setting would be as normal and not in an exceptional position.

Example 21

> … when the flight crew was preparing for landing, the main landing gear failed to extend following normal selection. While maintenance personnel were completing their checks of the aircraft following maintenance, the flight crew interrupted the task in order to expedite the flight. That resulted in the position of the main landing gear inhibit switch not being verified by maintenance personnel. When the flight crew prepared the aircraft for flight, they did not confirm the position of the main landing gear inhibit switch. … When the flight crew selected the landing gear to the down position (extended), the landing gear inhibit switch was in the INHIBIT position, thereby preventing normal extension. No caution advisories were illuminated. Had they been illuminated, the crew would have been directed to the ALTERNATE LANDING GEAR EXTENSION/ LANDING GEAR MALFUNCTION checklist and that would have led them to check the inhibit switch for position. … The BEFORE START

checklist used by the crew, did not have such a requirement.

ATSB occurrence No: 200105743

5.2.1.4 Fuel selection/ fuel management system

Functions

In order to prevent engine stop because of fuel exhaustion, fuel management systems in aircraft provide three systems to indicate fuel quantity; a manual check by putting a dipstick into a fuel tank, a fuel quantity indicator in cockpit displays, and a fuel log system that records fuel consumption in a written log.

Error modes

There are many cases of human error in managing aircraft fuel management systems. If there are differences in positions (see Figure 5.5), procedures etc. from previous experience, operators could fail to conduct correct procedures in the system (example 22).

In practice, the aircraft can be operated with the minimum fuel sufficient for safe flight in order to maximise payloads. Consequently, the fuel tanks would rarely have been filled to capacity. As filling the fuel tanks to capacity provides one of the only opportunities to accurately determine a datum for the assessment of fuel quantity, any subsequent inaccuracies in the system of assessing fuel quantity would have compounded over extended periods. In example 22, as most of the pilot's previous flying experience had not involved working in situations where it was necessary to carefully balance the requirements of payload against fuel, it is possible that he did not recognise the critical need to carefully monitor such aspects of the operation (examples 23, 24),

A Fuel Selector System requires a specific procedure. In example 25, two fuel selector controls were attached to the cabin floor between the pilot and co-pilot seats. The selectors enabled the fuel selector valves, located behind the engine firewalls, to be positioned to the corresponding tank, crossfeed, or off. In the Normal Procedures section of the handbook, pilots were cautioned that they should "Feel for (the) detent" when placing the fuel selector at the desired position. The operator's standard operating procedures required pilots to operate the fuel supply cross feed for 60 seconds to verify normal operation. Also, pilots were to ensure normal operation of the fuel valves by positioning the fuel selectors to the off position to observe a decrease in fuel flow. The fuel system pre-flight checks specified in the operator's Cessna 402C Operations

Manual differed from the procedures specified in the manufacturer's Pilot's Operating Handbook.

Example 22

> At impact, the left propeller was in the feathered position and fuel to this engine had been shut off. … The investigation revealed that, apart from a 2-hour flight the previous day, the pilot had no other experience in SPP. It was also revealed that there were two significant differences between the fuel system in SPP and that of other Aero Commander models the pilot had flown. These differences concerned the time taken for the outboard fuel tanks to empty and the orientation of the cockpit fuel selector switches. The analysis concludes that these differences probably led to mismanagement of the fuel system by the pilot and to failure of the left engine due to fuel starvation, followed a short time later by failure of the right engine, also due to fuel starvation. *ATSB occurrence No:*199403314

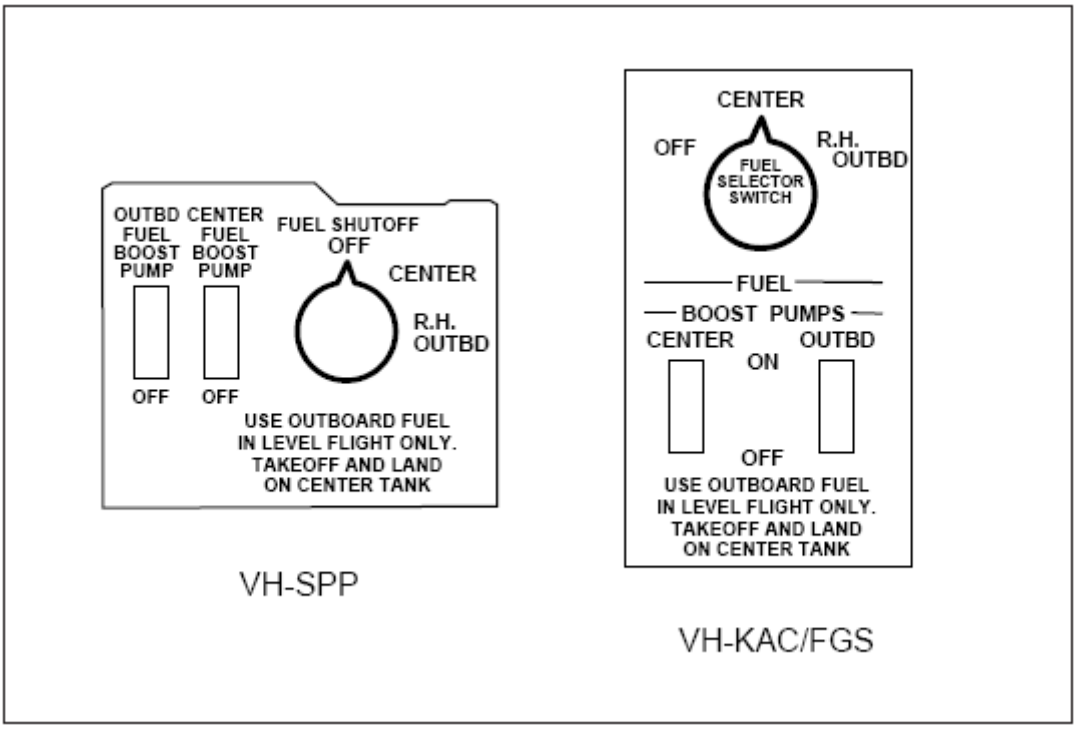


Figure 5.5 A sketch of comparison of the fuel control panels for SPP and KAC/FGS (for example 22)

Example 23

> There were two systems available to a pilot to monitor fuel quantity - a fuel quantity indicator and a fuel log. The fuel quantities as determined by each system should have been in agreement. During the accident flight, however, the pilot had covered the fuel gauge due to intermittent and unreliable fuel indications, which made one system unusable. In addition, the fuel-log system was not being applied with rigour and did not provide an accurate indication of the actual fuel quantity. This had masked any opportunity to reveal differences in estimated and actual consumption rates, when compared with the fuel gauge. As a result, at the time of the occurrence the aircraft had substantially less fuel on board than the pilot believed to be the case. *ATSB occurrence No:*199804432

Example 24

> The checks conducted by the pilot prior to the flight were inadequate to the extent that the pilot significantly over-estimated the quantity of fuel available for the flight. The right engine failed due to insufficient fuel in the right tank while the aircraft was in a climb attitude. … The pilot apparently over-relied on the tachometer and manifold pressure gauge indications, but lacked an understanding of those indications. *ATSB occurrence No:*200200047

Example 25

> The pilot did not move the fuel selectors to the off position as part of the pre-flight checks. This was because the Fleet Manager had advised his intention to amend the pre-flight check to delete the requirement. … The manufacturer's Pilot's Operating Handbook did not specify checks for crossfeed operation or positioning the fuel selectors to the off position to observe a decrease in fuel flow. *ATSB occurrence No:* 200001827

5.2.1.5 Warning systems

In order to avoid unexpected events, such as collision with other aircraft or depressurisation, some systems, such as TCAC, have been designed.

TCAC system

Functions

The Traffic Alert and Collision Avoidance System (TCAS) is a computerised avionics device which is designed to reduce the danger of mid-air collisions between aircraft. It monitors the airspace around an aircraft, independent of air traffic control, and warns pilots of the presence of other aircraft that may present a threat of mid-air collision.

Error modes

There may be specification of time to warm up before the operation of a transponder for TCAS. If this specification of design has no plan to achieve the procedure before the operation, it may fail to do it (example 26). A state of operator's cognition at the time of a traffic alert is highly demanding. In this condition, a human operator has no time to conduct a knowledge-based performance. Unclear direction may lead to an operator misunderstanding the message (example 27).

Example 26

> The operator instructed pilots to ensure that aircraft transponders are selected "On" and warmed up for five minutes before departure. *ATSB occurrence No:*200104280

Example 27

> As the 737 descended towards FL220, the crew was faced with the apparently conflicting demands of an ATC clearance and a TCAS resolution advisory. Given that the 737 was above the Brasilia, it would be normal for the initial TCAS advisory to have been a `reduce descent' or a climb advisory. … It is possible that the crew may have misidentified the TCAS aural warning. Prompt action was required to resolve the apparent ambiguity and the crew may have been guided more by the aural warning than by the IVSI display. That may have been, at least in part, due to the limitations of the IVSI display, where a pilot may initially rely more on the aural alert. Compared with a TCAS IVSI display, traffic information that is displayed on an EFIS screen increases the crew's situational awareness.

> However, pilots are trained to use all the information at their disposal and an aural alert would be the trigger to look at the IVSI display immediately. Therefore if the green band of the IVSI was indicating a required rate of descent of 1200-1500 ft/min, then the correct procedure would be to disengage the autopilot and smoothly adjust the pitch to attain that rate of descent. … Since the incident, the operator's TCAS software has been updated to Version 7. The objectives of the Version 7 update were to further increase the safety benefits of TCAS, make TCAS more compatible with the procedures used by ATC and to address operational concerns identified by pilots operating the older versions of TCAS. Improvements to the aural annunciations included a change from `reduce descent, reduce descent' to `adjust vertical speed, adjust'. *ATSB occurrence No:*200201725

The cabin altitude warning system

Functions

When an aircraft enters higher altitudes than flight levels at normal pressure, the crew need to notice altitude in order to avoid depressurisation in the cabin.

Error modes

In example 28, the crew entered a higher flight level without noticing their altitude.

Example 28

> As the aircraft climbed through FL125, the flight nurse noticed that the passenger oxygen masks had deployed and conveyed that fact to the pilot. The pilot was unaware of the deployment and had immediately turned around to assess the situation. When he turned his attention back to the instrument panel, the pilot noticed that the cabin ALT WARN caption positioned on the glare-shield mounted Master Warning panel was illuminated. Both Master Warning captions were also flashing. … Some vital checklist actions from the PRE TAKE OFF checklist and the AFTER TAKE OFF checklist were not

completed by the pilot. … The non-standard clearance instruction, received soon after take-off, required re-programming of the GPS. That action captured his attention during the climb, and distracted the pilot from performing parts of the AFTER TAKE OFF checklist and the Transition Altitude Procedure. The pilot had expected the routine illumination of the green auto feather advisory annunciators during the takeoff and for part of the climb. Consequently he did not identify that additional green annunciators, in the form of the bleed air off indications, were illuminated. … The operator's instruction that permitted completion of the AFTER TAKE OFF check "as workload permits", allowed for postponement of a critical check on cabin pressurisation until well above 10,000 ft. Postponement of the AFTER TAKE OFF check also maintained the Auto Feather in an active state, and kept the green annunciator lights illuminated. … Signification factors 1. The pilot did not complete the Pre Take Off and After Take Off cabin pressurisation checks. 2. The pilot became pre-occupied with programming the GPS after receiving a track change instruction. 3. The aircraft was allowed to climb above 10,000 ft in an unpressurised state. 4. The effectiveness of the aircraft's cockpit warning system was reduced by the operator's practice of allowing postponement of the After Take Off check. … *ATSB occurrence No:* 200105188

An Australian Transport Safety Bureau investigation into a Beechcraft King Air 200 depressurisation incident, BO/199902928, issued three recommendations on the subject of cabin alert aural warning systems. The final report contained an additional recommendation on the same subject.

Recommendation R20000288 stated: … "The ATSB therefore recommends that CASA mandate the fitment of aural warnings to operate in conjunction with the cabin altitude alert warning systems on all Beechcraft Super King Air and other applicable aircraft".

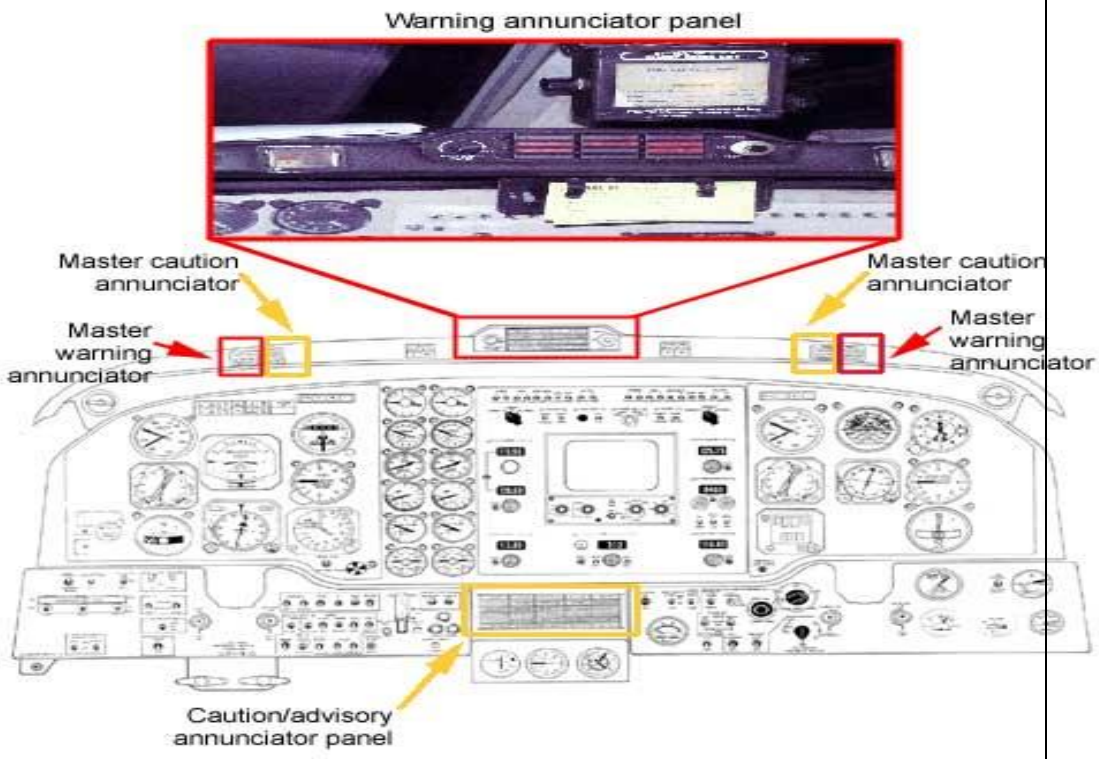


Figure 5.6 Beech 200 cockpit instrument panel layout, indicating caution, advisory and warning annunciators in example 28

The stall warning system

Functions

The stall warning system fitted to the Saab 340 consists of two independent dual channel stall warning computers, left and right angle-of-attack sensors, two stick shakers (one mounted on each control column) and a stick pusher actuator connected to the left control column. A mechanical linkage also transfers the stick push to the right control column. There are stall warning lights on each of the pilot's instrument panels, and three amber stall warning system failure lights on the centre warning panel.

Error modes

In this case studied (example 29), the investigation found that despite being certified to all required certification standards at the time, the Saab 340 aircraft can suffer from an aerodynamic stall whilst operating in icing conditions without the required warnings being provided to flight crew. The investigation also found a number of other

occurrences involving Saab 340 aircraft where little or no stall warning had been provided to the crew while operating in icing conditions. This problem had been recognized and modified stall warning system in advanced models of the aircraft. The safety system has been mandated for aircraft operated in Canada. I found other incident of same type of the aircraft in aviation accident reports. (ASN, Saab 340B Hazelton Airlines, 28 June 2002, available at http://aviation-safety.net/database/record.php?id=20020628-0 , September 2006)

Example 29

> The crew interpreted this ice deposit as being less than that required for them to activate the de-ice systems on the wing leading edges, in accordance with the aircraft flight manual procedures. As the aircraft approached Melbourne the crew were instructed to enter a holding pattern … Shortly after the aircraft entered the holding pattern it suffered an aerodynamic stall … The crew was not provided with a stall warning prior to the stall. … a number of recommendations were made in 1998 and 1999 concerning flight in icing conditions and modifications to the Saab 340 stall warning system. *ATSB occurrence No:*199805068

Weather Radar

Functions

The colour weather radar fitted in aircraft has a radar antenna transmitting microwave energy in the form of pulses, which, if reflected off precipitation ahead of the aircraft, would be returned to the antenna. The radar beam is a narrow cone with a beam width of 8 degrees. The mount of energy reflected back to the antenna is converted into a colour code for presentation to the crew on their flight instruments. There are four colour codes directly related to precipitation intensity, ranging from black (no precipitation), green (minimum detectable moisture), yellow (medium moisture level), to red (strong to extreme moisture level).

Error modes

However, due to the system limitations, heavy rainfall could reduce the ability of the weather radar to provide a complete picture of the weather ahead. Attenuation may reduce reflected precipitation readings, which the weather radar interprets as an area of decreased rainfall. As a result, the colour could be downward. The colour displayed to

the crew may indicate a lower level of precipitation intensity than is actually occurring. In this case, what would normally be displayed as a red return (indicating strong to extreme rainfall rates, with the possibility of associated hail) is displayed as a yellow return.

Due to this limitation of the airborne weather radar and possibly the radar antenna setting, it is possible for the flight crew to misinterpret the depicted weather radar returns as seen in example 30.

Example 30

> The flight crew did not appear to understand the limitations of the airborne weather radar. The aircraft was inadvertently flown into an area of severe convective weather activity. The weather encountered by the crew was as forecast. Action taken by preceding aircraft confirmed the crew's expectation that they would have to divert to the left of track when en route. After leaving controlled airspace, the crew had to rely, for operational decision-making, on their interpretation of information derived from the airborne weather radar. … The crew incorrectly interpreted the radar display of green and yellow returns as being acceptable. However, the heavy precipitation and hail produced by the storm cell was likely to have resulted in significant attenuation of the radar beam. Attenuation would have reduced the ability of the weather radar to accurately depict the precipitation intensity. Further, the radar antenna setting of 3 to 4 degrees up, as reported by the crew, would have resulted in the radar beam scanning above the level at which the aircraft was flying, and into an area that was above the freezing level. It is likely that above that level the hail was dry. As such, it would have provided a low reflectivity target for the weather radar, and may have contributed to the inability of the radar to provide the crew with an accurate picture of the precipitation intensity. … with inadequate radar derived information, the crew did not recognise the significance of the convective weather, and the aircraft entered the storm cell. *ATSB occurrence No:*200201228

GPS system

Functions

GPS refers to the Global Positioning System (GPS) which utilise a constellation of orbiting satellites that transmit precise microwave signals. The system enables a GPS receiver to determine its location, speed, direction, and time.

Error modes

Errors associated with GPS are found in highly workloads in this case studied. The problems associated with the procedure of GPS setting that can affect operators' cognition and performance did not well consider at the design stage. For example, case 31 shows that there was no design for detecting the limitations of GPS system that could lead to human error. The other cases 32 and 33 demonstrate that an additional work added to operators can confuse the operator. The GPS setting procedure did not consider that the procedure can take time and provoke cognition of operators. Just putting a procedure prompts for human operator to commit errors.

Example 31

> Due to errors in the Orion's navigation system, the aircraft failed to remain inside its assigned search area. The navigation errors were a function of equipment limitations and inadequate monitoring of the aircraft's position by the crew. Consequently the Orion crew inadvertently searched in the area assigned to the Cessna 402. At the time of the incident most members of the Orion crew were highly fatigued, having been awake in excess of 24 hours. *ATSB occurrence No:* 199805874

Example 32

> As the aircraft reached the cruise level of FL250, the controller contacted the pilot, indicating that the aircraft was not maintaining the assigned track. The pilot acknowledged this transmission. A short time later the passenger in the co-pilot seat noticed that the pilot was again attempting to program the GPS, and was repeatedly performing the same task. The controller advised the pilot again that the aircraft was still off track, however the pilot did not reply to this transmission. Shortly after this, the pilot lost consciousness. *ATSB occurrence No: 199902928*

Example 33

> Following take-off, at about 2,000 ft, the air traffic controller instructed the pilot to intercept the 173 radial at 120 NM from Tindal, and then to track along that radial to Tindal. That had been necessary to avoid the now active Military restricted area R248(B). The pilot reported that he had then become occupied with re-programming the aircraft's Global Positioning System (GPS). During the climb to the cleared level, Flight Level 130, the pilot reported that he believed that he had actioned all the required checklist items. *ATSB occurrence No: 200105188*

5.2.1.6 Monitoring systems

Functions

The crew or controller should monitor developing situations.

Error modes

In example 34, a distraction occurred as a crew member monitored the weather radar and assessed the meteorological conditions that the aircraft was encountering during the climb. At the time of the infringement, the B737 was being manually flown by the pilot in command who was distracted from his primary task of controlling the aircraft's flight path.

When there are two systems with the same value, it may confuse people to identify which is being used. For example, a unit of weight may be either in imperial or metric units. People involved in checking or converting such units of measurement may make errors. (example 35)

Example 34

> After take-off, the B737 entered cloud and encountered turbulence as it climbed through 3,500 ft. The pilot in command was monitoring the aircraft's weather radar and stated that he became distracted while assessing the meteorological conditions. Although the co-pilot gave the 1,000 ft to assigned altitude call at 4,000 ft, he was also observing the weather situation and did not monitor the flight

instruments as the aircraft approached the assigned altitude. *ATSB occurrence No:*200200463

Example 35

When the agent who handled freight at Honolulu for the B767 operator received the pallet weights, she did not check the figures against the loadsheet issued by Load Control. Consequently, she did not realise that the weights stated on the loadsheet had already been converted to kilograms, and applied the conversion a second time. Also, as the agent for the US operator was confident that she had passed the correct weights to the B767 agent, she did not recheck to ensure that the B767 agent had received the correct weight information. The 220 kg and 10 kg weight discrepancies affecting the other two pallets were probably the result of weighing or recording errors. *ATSB occurrence No:*200100596

5.2.1.7 Traffic communication system

It is necessary to communicate among controllers and pilots in aviation. The general method of communication between an air traffic controller and a pilot is voice radio, using either VHF bands for line-of-sight communication or HF bands for long-distance communication. One of the major problems with voice radio communications used in this manner is that all pilots being handled by a particular controller are tuned to the same frequency. This increases the chances that one pilot will accidentally override another, thus requiring the transmission to be repeated. (Wikipedia, Novenber 2007, http://en.wikipedia.org/wiki/CPDLC) There has developed many communication systems in order to improve efficiency in communication and reduce burdens of people involved in communication.

Controller Pilot Data Link Communications (CPDLC)

Functions

Controller Pilot Data Link Communications (CPDLC) is a method by which air traffic controllers can communicate with pilots over a datalink system. CPDLC is a data link application that allows for the direct exchange of text-based messages between a controller and a pilot. CPDLC greatly improves communication capabilities in oceanic areas, especially in situations where controllers and pilots have previously had to rely on a Third Party HF communications relay. Apart from the direct link, CPDLC adds a

number of other benefits to the ATS system, such as; allowing the flight crew to print messages; allowing the auto-load of specific uplink messages into the Flight Management System (FMS); allowing the crew to downlink a complex route clearance request, which the controller can re-send when approved without having to type a long string of coordinates. [ATC data link news, http://members.optusnet.com.au/~cjr/CPDLC.htm].

Error modes

The preformatted message function in CPDLC helps to reduce the crew's workload. That was reported to be a common practice and assisted with workload management. Pre-formatted messages configured in the system such as seen in example 36 and 37, however, could be sent without careful checking by operators, especially if there was some change in situations. Operators who have used computerised systems tend to rely on the system (example 38).

Example 36

> The controller intended to send the message to the crew of the north-east bound B747 once they had passed the south-west bound B747 and a separation standard had been established. However, he unintentionally sent the message before the two aircraft had passed. … The air traffic controller had planned to assign FL350 to the crew of the north-east bound B747 to maintain a separation standard with a third B747 travelling on B200 at FL330 in the opposite direction. However, FL350 was not available to the north-east bound B747 crew until the controller in Tahiti could established a separation standard with the south-west bound B747 travelling in the opposite direction at FL340. … The controller had prepared a pre-formatted controller-pilot data link communication (CPDLC) message for transmission to the crew of the north-east bound B747. … However, he unintentionally sent the message before the two aircraft had passed. *ATSB occurrence No: 200200190*

Example 37

> … the crew of OED then contacted Tahiti ATC via HF radio and advised that they could reach FL350 by time 1140 universal coordinated time. The controller responded via HF radio and instructed the crew of OED to maintain FL330. The crew of OEB then requested, via CPDLC, climb to FL330. The CPDLC response provided to the crew of OEB was 'climb to and maintain FL330 due to traffic' even though FL330 was not available. The message was selected by the controller from the menu of pre-formatted messages available in the system. The controller had not intended to assign FL330 to the crew of OEB and did not realise that they had been assigned FL330, or that they had climbed to FL330 and subsequently returned to FL320. *ATSB occurrence No:* 200200094

Example 38

> The flight crew and controller were communicating via controller-pilot data link communications (CPDLC). The crew requested approval to climb to and operate between FL290 and FL330. The controller sent an approval at 0659 on the CPDLC for the crew to climb to the block level. … The B747 crew maintained their aircraft at FL290 and immediately reported via the CPDLC that they were unable to comply due to traffic. This message was sent at 0659 but was not received at the controller's terminal until 0706. The delay was believed to be due to network lag. The traffic was subsequently identified as a British Aerospace 146 (BAe 146), en route from Norfolk Island to Sydney at FL310. … The controllers' understanding of the operation of the CPDLC appeared to be limited and it was this aspect, in conjunction with an inadequate appreciation of the potential conflict, that led to the occurrence. Once the controller recognised that the approval message had not been placed on hold, HF radio should have been utilised to ensure the B747 crew were to maintain FL290, rather than rely on the CPDLC. Any delay to the crew receiving this instruction may have compromised the safety of the two aircraft. *ATSB occurrence No:*199804129

Radio Communications

Error modes

In example 39 the deficiencies related to the depiction of holding patterns on en-route charts, the appropriateness of the use of non-standard holding patterns, and associated radiotelephony phraseology may lead to error of misunderstanding between the pilot and controllers.

In the case 40, the air traffic controller had insufficient time to establish communications with both crews and provide them with sufficient information to enable them to take action to prevent a near collision.

Example 39

> Air traffic control had issued the crew of a foreign Boeing 767 (B767) with an instruction to hold at Bindook. Although the published holding procedure required a left pattern, the crew turned the aircraft for a right pattern. The right turn subsequently placed the aircraft into conflict with a Boeing 747, which was being radar vectored to the south of Bindook. … An investigation revealed that the crew did not locate the holding pattern on the Jeppesen terminal chart. The depiction of the holding pattern was difficult to distinguish from other markings on the chart and the pattern was not displayed on the appropriate Standard Arrival Route (STAR) chart. In addition, the holding pattern was not loaded in the aircraft's flight management computer database. The Captain of the B767 reported that in the USA, where a holding pattern is not displayed, or in the absence of other information, a "default" right hand pattern is to be flown. There is no such procedure in Australia. As a result, the Captain elected to fly a right hand pattern without checking with air traffic control for holding pattern information. *ATSB occurrence No:*199803921

Example 40

> The crew of the Jetstream did not hear the King Air crew's inbound broadcast on the mandatory broadcast zone frequency. The crew of the King Air did not hear the Jetstream crew's taxi broadcast on the mandatory broadcast zone frequency; nor did they hear the transmissions made on the

> Brisbane control frequency by the air traffic controller that provided essential traffic information regarding the Jetstream, and instructed them to maintain 6,000 ft. *ATSB occurrence No:* 199805078

Air traffic control instructions

Error modes

In example 41, the instructions of the local air traffic controller at Cairns (Queensland) stated that a clearance to aircraft to track via the "southern shores" was meant to provide wake turbulence separation between an aircraft departing Cairns via a runway 15 SID and an aircraft over the southern shore of the Cairns inlet. A term not correctly defined may lead to error of interpretation of the term.

Example 41

> The controller issued a clearance to the pilot of the Cessna that was, to the aerodrome controller, a specified route but one that was not known to the pilot. The aerodrome controller was not aware that the pilot's understanding of the 'southern shores' differed from his own. The meaning of the term 'southern shores' was not available to the pilot of the Cessna and therefore the potential existed for the misunderstanding between the pilot and the aerodrome controller that resulted in this occurrence. *ATSB occurrence No:* 200202385

5.2.1.8 Procedure/ emergency procedure

Simultaneous opposite-direction parallel runway operations (SODPROPS)

Functions

SODPROPs refers to one specific method of coordinating the arrival and departure of planes. In a situation where there are two parallel runways, it means that planes are arriving on one runway and departing from the other at the same time. This method of operation has developed to utilise runways and increase flight departures and arrivals. (Airspace, http://www.newparallelrunway.com.au/content/standard1.asp?name=Airspace_faqs).

Error modes

The process is very fast so operators involved in the system that cannot easily reverse or correct a procedure when a mistake happens (example 42).

Example 42

> The crew mistakenly dialled 155 degrees into the aircraft's flight control unit (FCU) on the glareshield as the aircraft lined up on the runway, but correctly acknowledged to air traffic control (ATC) the assigned heading of 115 degrees. After takeoff, … The aerodrome controller saw that the A320 did not turn left as instructed, but as the crew had already transferred to the departures south (Departures (S)) frequency, he was not able to instruct them to turn left onto the correct heading. … The SODPROPS procedure was introduced to the Sydney Airport environment with neither the regulator nor the airservice provider having adequately analysed the risks associated with the implementation of the standard. *ATSB occurrence No:* 199700052

Blanket clearance

Functions

Blanket clearance allows aircraft to occupy or cross a runway without a specific clearance from the ADC. The use of a blanket clearance reduces the need for segmented taxi clearances.

Error modes

In this case studied (example 43), the controllers did not conduct an effective scan of the runway. They were distracted by other tasks. The blanket clearance departure procedure negates a safety defence by reducing time, eliminating one safety check procedure.

Example 43

> The local procedures in the Adelaide tower for a blanket clearance of a runway release required the use of a bright yellow coloured flight progress strip with the words "RUNWAY 12/30 OCCUPIED". Although a strip was correctly placed in

> each of the strip presentation bays in front of both the SMC and the ADC to indicate that a blanket clearance was issued, that procedure failed to attract the attention of the ADC. …The ADC did not conduct an effective scan of runway 30 or the flight progress strip display prior to clearing the Pilatus to take off. The presentation of the yellow flight progress strip did not alert the ADC that a runway 12/30 blanket clearance was in place. The ADC did not hear the SMC issue a clearance for the crew of the B737 to cross runway 30, nor did the SMC hear the ADC issue a take-off clearance to the Pilatus. The ADC did not observe the B737 moving towards runway 30. The SMC was distracted from a surveillance role by other tasks. *ATSB occurrence No* 199804069

Emergency procedure

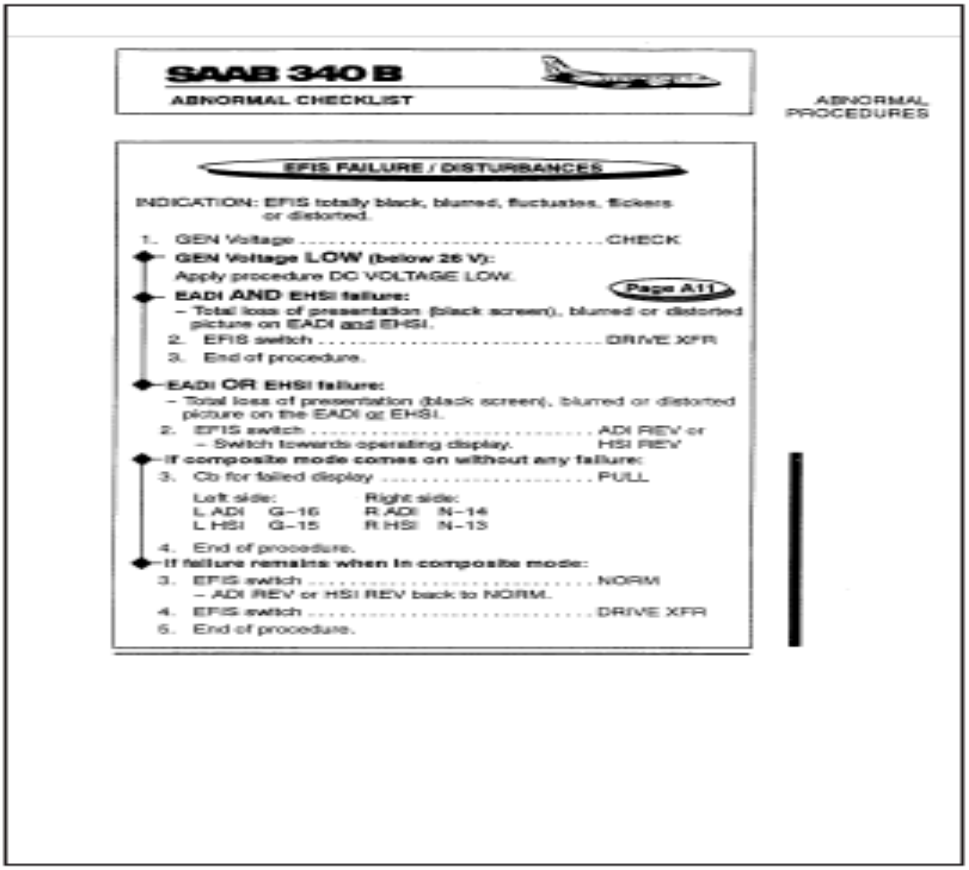
Error modes

A state of emergency (e.g. failure of some systems) makes operators become involved in a hectic situation. According to psychological studies, their perception and reasoning models are very restricted compared with their normal state. In the case of example 44, the crew did not find the reason for the failure of the electronic flight information system (EFIS) screens. They then omitted the first item of the emergency checklist (see **Figure 5.7**) for EFIS failures. One reason for their oversight may be that there was no reasonable relationship between the observed DC starter generator failure and the symptom of EFIS failure. There was no alert for generator failure. Example 45 shows that performances of operators in a state of emergency are not always logical, contrary to what designers assume.

Example 44

> While on climb through FL180, the copilot's two electronic flight information system (EFIS) screens on the right side of the aircraft's instrument panel failed. After the crew had consulted the EFIS failure/disturbances checklist, the central warning panel ice protection annunciator and then the cabin pressure annunciator illuminated. … During the investigation it became apparent that in some Saab 340 aircraft a starter generator could fail without taking the generator off line and alerting the crew, resulting in low system voltage. On this

occasion the crew overlooked the first item of the EFIS failure/disturbances checklist, which required a check of the generator voltage. Consequently, the crew did not recognise the developing low voltage condition that led to the cascading series of warnings, cautions and failures. …This occurrence also demonstrates the need for well-designed checklists to be available to pilots during abnormal or emergency situations. It further demonstrates the need for pilots to be familiar with the systems of the aircraft they operate and the actions to be taken in the event of abnormal or emergency situations. The investigation determined that the modification to reduce the risk of the consequences of a delayed generator failure warning was highly desirable. *ATSB occurrence No:* 200105715



SAAB 340 B

ABNORMAL CHECKLIST

ABNORMAL PROCEDURES

EFIS FAILURE / DISTURBANCES

INDICATION: EFIS totally black, blurred, fluctuates, flickers or distorted.

1. GEN Voltage ..... CHECK

GEN Voltage LOW (below 25 V):

Apply procedure DC VOLTAGE LOW.

EADI AND EHSI failure:

– Total loss of presentation (black screen), blurred or distorted picture on EADI and EHSI.

Page A11

2. EFIS switch ..... DRIVE XFR
3. End of procedure.

EADI OR EHSI failure:

– Total loss of presentation (black screen), blurred or distorted picture on the EADI or EHSI.

2. EFIS switch ..... ADI REV or HSI REV
   – Switch towards operating display.

If composite mode comes on without any failure:

3. CB for failed display ..... PULL

Left side:		Right side:	
L ADI	G–16	R ADI	N–14
L HSI	G–15	R HSI	N–13

4. End of procedure.

If failure remains when in composite mode:

3. EFIS switch ..... NORM
   – ADI REV or HSI REV back to NORM.
4. EFIS switch ..... DRIVE XFR
5. End of procedure.

Figure 5.7 EFIS failure/disturbances checklist (in example 44)

Example 45

> The flight attendant did not don an oxygen mask during the incident. … The procedures permitting discretionary use of supplemental oxygen following activation of the cabin altitude warning system did not recognise that, in some circumstances, the crew's decision-making may already have been impaired. The response to such a warning should take that factor into account. The aircraft manufacturer's QRH checklist (following an illumination of the cabin altitude warning light) did not include a checklist item for the crew to don oxygen masks, potentially exposing them to the effects of hypoxia while performing the checklist items. *ATSB occurrence No:*200003725

Flight plan system

Error modes

In example 46, the flight plan for the A320 included a manoeuvring time for the aircraft prior to setting course. The air traffic control strip printing system was unable to allow for a discrete manoeuvring time in the strip preparation. The Melbourne Sector 4 controller did not conduct a cross-check calculation on the flight progress strip notation for the A320's estimated time of arrival at SUBUM.

Example 46

> The Adelaide Sector 4 controller checked his flight progress strips and noticed that the A320 was early at Portland but estimated to be "on time" at SUBUM. He considered that this discrepancy was probably due to a flight planning error that had been corrected by the Melbourne controller. … The air traffic control strip printing system's interpretations of the A320's flight plan led to a latent error in the flight progress strips for the A320 that was not present in the B737 strips. *ATSB occurrence No:* 199702620

The runway 15 SWIFT standard instrument departure

Functions

The SWIFT 2 standard instrument departure was designed to counter the limitations of high terrain surrounding Cairns airport and the tracking requirements of inbound aircraft from the south and east. The procedure required crews to turn their aircraft at the earlier of 400 ft or the departure end of the runway and then track to 030 degrees until climbing through 4000 ft. At that point the aircraft should be turned right onto a track of 170 degrees M to intercept the 139 degrees radial of the Cairns VOR (VHF navigation aid).

Error modes

In this case studied (example 47), both crews had been cleared via the runway 15 SWIFT 2 standard instrument departure. The performance of the B737-400 series aircraft was superior to that of the B737-300 series aircraft. CZC, the B737-300 series aircraft, had taken 1 minute 56 seconds to reach 4000 ft whereas TJW, the B737-400 series aircraft, took only 1 minute 27 seconds to pass the same altitude. However, controllers thought that the aircraft were “like types” for the purposes of departure standards. The procedure allowed the possibility of a following aircraft turning inside a preceding aircraft. The use of minimum departure separation standards was inappropriate.

Example 47

> The approach/departures controller had approved a request for a change of level from a pilot of an aircraft that had departed Cairns approximately 7 minutes earlier. After issuing the departure clearances, the controller commenced the process of making the change in the air traffic computer; an action that required nine clicks of the mouse. In order to make this change, the controller looked away from the air situation display (which was on the main screen) and used the auxiliary screen to observe the flight plan window while using the keyboard to input the data. … The performance of the B737-400 series aircraft was superior to that of the B737-300 series aircraft. Controllers at Cairns considered that the aircraft were "like types" for the purposes of departure standards … The design of the SWIFT 2 standard instrument departure did not guarantee separation assurance. Whenever the second aircraft reached 4,000 ft prior to the first aircraft (whatever the

reason) a reduction in horizontal separation was likely. *ATSB occurrence No:* 199902003

V1 cut procedure

Functions

It is one of take-off techniques. The V1 cut procedure itself required precise control of the aircraft. Aircraft performance would have been rapidly eroded if the attitude was not set accurately and if appropriate yaw and roll inputs were not made. It was important to retract the landing gear early to reduce drag.

Error modes

The crew assumed that the procedure is permitted. Interpretation of the procedure was different from that of the designers (example 48).

Example 48

During the briefing prior to the second flight, the check-and-training pilot indicated that he would give the co-pilot a V1 cut during the takeoff. The co-pilot questioned the legality of conducting the procedure at night. The check-and-training pilot indicated that it was not illegal because the company operations manual had been amended to permit the procedure. … an inadequate Metro III endorsement training syllabus in the company operations manual; *ATSB occurrence No:*199503057

Minimum equipment list (MEL)

Functions

MEL refers to minimum equipment list. MEL list is a categorized list of instruments and equipment on an aircraft allowing it to be operated with some of those instruments or pieces of equipment inoperative. In this case studied, the aircraft departed with a MEL 36-11-07 restriction applied following the failure of the right engine high-pressure valve (HPV). Part of the MEL restriction required that the right engine bleed-air HPV be locked in the closed position by a locking pin. The operation of the engine HPV normally supplemented the bleed-air supply to the aircraft at low engine speed. At

higher engine speeds, such as occur during normal flight, the bleed-air system was supplied with enough air to operate the airconditioning pack, even with the HPV locked closed. The MEL was part of an operator-customised publication, which had been developed from the aircraft manufacturer's master MEL. Part (b) of the "Operations" section of the operator's MEL stated:

(1) At low engine power (around idle thrust) setting:

(a) Associated bleed is selected OFF.

Error modes

Example 49 demonstrates how an ambiguous phrase in the instruction for the MEL operation leads pilots into misinterpretation of the instruction. The MEL was part of an operator-customised publication, which had been developed from the aircraft manufacturer's master MEL but differed from it in wording.

Example 49

> While cruising at Flight Level (FL) 370 on a flight from Perth to Adelaide, the crew of the Airbus A320 noticed that the left engine bleed-air fault warning had illuminated. The aircraft pressurisation and airconditioning systems then automatically shut down, and the cabin pressure altitude began to increase at approximately 700 ft per minute. The crew made an unsuccessful attempt to reselect the left engine bleed air to on, and the aircraft auxiliary power unit (APU) was started. … The crew interpreted the operator's MEL to mean that at engine "idle thrust" they were to turn the bleed air from that engine to off. That prevented any supply of bleed air for the pressurisation and airconditioning system coming from that engine. They then opened the bleed air cross-bleed valve and operated both airconditioning packs from the right engine only. … Since the occurrence the operator has amended and strengthened the contents of the operations area of MEL 36-11-07 to reflect the intention of the manufacturer's MMEL. This was done to "reduce the possibility of incorrect system operation with one HP bleed source inoperative". *ATSB occurrence No:*200003533

The emergency power lever (EPL) procedure

Error modes

In this case studied (example 50), the pilot's operating handbook (POH) contained a requirement to place the engine ignition switch in the ON position during an actual malfunction of the fuel control unit (FCU). However, because the aircraft manufacturer only included requirements for an actual FCU malfunction, the POH did not address the engine control settings for training of this type.

The pilots assumed that the use of the EPL for familiarisation training in-flight was acceptable. Their assumption was based on there not being a description of prohibition for the procedure in the manual.

Example 50

> The pilots of CYC were conducting in-flight simulated engine failure training, which involved activation of the emergency power lever (EPL). The engine ignition switch was not in the ON position during the initial operation of the EPL during this training. The POH contained a caution which stated that the use of the EPL was for emergency purposed only, and did not mention the use of the EPL for in-flight or ground familiarization training. The engine manufacturer's Service Information Letter (SIL) noted the use of the EPL for familiarization training, while suggesting that this training be completed on the ground. The discrepancy between these two documents may have led to the flight crew's belief that the use of the EPL for familiarization training in-flight was acceptable.
>
> That procedure was not contained in the aircraft manufacturer's pilot operating handbook. However, the engine manufacturer's documentation contained information on the use of the emergency power lever, which did not preclude the use of the emergency power lever for in-flight familiarization training. *ATSB occurrence No:*200400443

5.2.1.9 Wire detecting system

Functions

There are lots of wires (e.g. power lines) crossing plains and over mountains and hills. Sometimes it is difficult for pilots to notice or identify the power cable lines due to unclear distinction of cable lines from the air. When an aircraft needs to fly low near wires, the wire strike protection system (WSPS), helps pilots to identify objects in order to avoid collisions.

Error modes

In example 51, wires were aligned on 060 degrees magnetic, with a maximum height of 31.5 metres for the upper wire and 30.1 metres for the lower wire. The position of the wires was not annotated on the relevant Visual Terminal Charts and they did not have high visibility devices attached. The pilot did not notice the wires. There was not a WSPS fitted to the helicopter.

Example 51

> The pilot of a Bell Long Ranger 206L-1 was returning to base following an agricultural crop-spraying task. While transiting a ridgeline of the Connors Mountain Range, the helicopter collided with wires and impacted the ground in a densely wooded area about 200 metres beyond the wires. *ATSB occurrence No:*200100443

5.2.1.10 Runway safety system

In order to prevent conflict in departure, landing or taxiing of aircraft from obstructions on runways, air traffic controllers (aerodrome controllers (ADC), departure controllers, approach controllers and surface movement controllers (SMC)) should cooperate with each other.

Functions

Supportive devices for controllers to recognise the situation of runways have been developed. Designation signs and strips are the most common systems of runway safety systems. For example, in example 52, there was a runway selection system. The procedure for release of the runway from the ADC to the SMC was for both the ADC and SMC to de-select their respective runway selection buttons for the appropriate

runway. Both buttons would become illuminated when selected, indicating that the runway was active. De-selecting each button had the reverse effect. Should the button be selected or de-selected on one side only, both lights would flash to alert the controllers to a mismatch.

Error modes

There were ten cases of runway safety failures in this study. In order to utilise runways for taking increasing quantity of traffic, runway systems have become complicated. There are many runways that cross each other. That makes it difficult for controllers to monitor runways continuously. When there are other people involved in scanning runways, operators can easily assume other colleagues have done the scan and make no further check (example 52).

In order to prevent conflict in runway between aircrafts and cars, designation systems are provided. However, it is an arbitrary system to change strips. In example 53, the ADC did not change the “runway designator” strip to indicate that Car 23 had entered the runway. The ADC did not adequately scan the runway prior to issuing a landing clearance to the crew of WBA. If there is no effective memory makers to help operators to recognize situation the operators may make errors (example 54).

Example 52

> The crew of a Metro 23 was cleared by the surface movement controller (SMC) at Perth to enter runway 11 and taxi to the threshold of runway 21 prior to departure. However, as the aircraft approached the runway 11 holding point, the crew checked the final approach path and saw a Cessna C402 landing on runway 11 in front of them. … The SMC did not conduct an effective scan of the airfield prior to advising the ADC of "no traffic". The ADC did not conduct an effective scan of runway 11 or the flight progress strip display prior to clearing the C402 to land. The flight progress strip display, and the controller's management of the console, did not provide the controllers with an accurate representation of the traffic situation. The airfield layout increased the potential for a runway incident. *ATSB occurrence No:*199803910

Example 53

> Although he scanned the runway prior to clearing WBA to land, the aerodrome controller did not expect to see a vehicle, as he was aware that the tractors were no longer obstructing the runway. Both strips had been in the bay for some time, which could have served to further diminish possible recall that Car 23 was now on the runway. It is also likely that the white colour of Car 23 made it difficult to see against the background of white runway markings or white gable markers. Consequently, without an effective alert to the presence of the vehicle on the runway, the controller's scan was inadequate to see Car 23. *ATSB occurrence No:*199804072

Example 54

> After landing on runway 27 at Melbourne during land and hold short operations, VH-CZH, a Boeing 737, vacated the runway via the parallel taxiway Echo which crossed runway 34 at a distance of 2,333 m from the threshold. The surface movement controller instructed the crew to hold short of runway 34 because VH-OGK, a Boeing 767, was landing. …VH-EAL, a Boeing 767, was taxiing for a runway 34 intersection departure at taxiway Juliet, 773 m from the runway 34 threshold. The aerodrome controller did not scan runway 34 before issuing the take-off clearance. There was no tactile memory marker alerting the controllers that an aircraft had been cleared to cross an active runway. *ATSB occurrence No:*199803972

Localiser

Functions

The Instrument landing system (ILS) is a ground-based instrument approach system which provides precise guidance to an aircraft approaching a runway, using a combination of radio signals and, in many cases, high-intensity lighting arrays to enable a safe landing during Instrument meteorological conditions (IMC), such as low ceilings or reduced visibility due to fog, rain, or blowing snow. An ILS consists of two independent sub-systems, one providing lateral guidance (Localizer), the other vertical

guidance (Glideslope or Glide Path) to aircraft approaching a runway. Aircraft guidance is provided by the ILS receivers in the aircraft by performing a modulation depth comparison. The localizer provides for ILS facility identification by periodically transmitting a 1020 Hz morse code identification signal. (Wikipedia, http://en.wikipedia.org/wiki/Instrument_Landing_System, November 2007)

Error modes

Crews of aircraft with advanced technology are required to exercise extreme caution in tuning and identifying navigation aids to ensure that the correct navigation aid frequency has been selected. However, it is difficult for humans to concentrate their attention on clearly identifying frequencies every time. Operators have a possibility of failing in setting numbers or signs in the system. Depending on the configuration of the selected navigation display mode, there may be insufficient cues displayed which would alert the crew that an incorrect navigation aid has been manually selected (example 55).

Example 55

> Both pilots incorrectly tuned the Cairns runway 33 localiser on 109.5 MHz instead of the runway 15 localiser on 109.9 MHz and subsequently misidentified the morse-code identifier. Their errors represented inadvertent failure to carry out routine and highly practised tasks. The crew had operated into Cairns the previous night and on that occasion the runway 15 localiser was not operating properly. On the night of the occurrence, although both pilots had the incorrect frequency selected for the runway 15 localiser, they incorrectly assumed the localiser was still experiencing service difficulties. This assumption arose because neither crew member was receiving a glideslope indication on his flight instruments. …. As a result of this occurrence, the ATSB (formerly BASI) issued Safety Advisory Notice SAN19990083 concerning un-notified back beam radiation from a localiser. The safety deficiency noted that back beam radiation from a localiser may give false course indications if the navigation aid frequency is inadvertently selected for an approach. There are no published procedures for the conduct of a precision approach using course guidance from a LLZ back beam. However, it is possible for an aircraft intercepting the back beam of the LLZ

for runway 33 at Cairns (identifier ICN, frequency 109.5 MHz) when making a LLZ approach to runway 15 at Cairns (identifier ICS, frequency 109.9 MHz), if the incorrect approach aid frequency is manually selected. Other locations within Australia where similar localiser configurations exist may cause similar problems. *ATSB occurrence No:*199902874

5.3 Diagram Analysis

How can the meta-theory of design-induced error help people to identify implicated design concepts and affected forms of human errors?

Is there any way to represent relationships between design and human error in accident reports?

The concept of design-induced error means to pursue relations between design and human error. However, it is not easy to find such relationships in an accident because contributory factors such as influences of design on human errors may be not well noticed during investigation of the accident and hardly recorded as having a direct relationship in the accident reports. Therefore, analysts should investigate and analyse accident reports thoroughly. This takes effort and is time consuming.

In order to facilitate understanding design issues in human errors from accident cases, many methods have been developed. Diagrammatic methods could be useful tools for the purpose. For example, Jun [2007] presents results of ten methods (i.e. stakeholder diagram method, information diagram method, process content diagram method, flowchart method, swim lane activity diagram method, state transition diagram method, communication diagram method, sequence diagram method, data flow diagram method, and IDEF0 method) of analysing a questionnaire on people who work in the healthcare sector. He found the flowchart diagram method was the easiest method to understand and most helpful in clearly understanding care processes and analysing task-related hazards.

This section presents analysis results with a concept of design-induced error and a diagram method that has been modified from the V^2 analysis method.

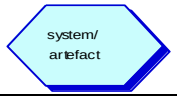
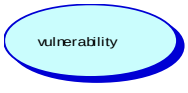
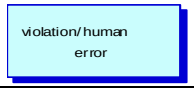
5.3.1 Method

The V^2 analysis method was chosen for diagram analysis. The Violation and Vulnerability (V^2) analysis method has been suggested for analysing the root cause of safety-related incidents and accidents [Johnson, 2005]. Among other event-based techniques for safety analysis [Livingston et al., 2001], V^2 focuses on using diagram to reveal hidden relations between violation and vulnerability. For systematic examination of specific findings the method involves finding the related probable causes and contributing factors to an accident [Johnson, 2005. The method provides depiction of

the arguments that connect the findings and evidence with diagrams. It takes descriptions from accident reports and then shows relations between violation (e.g. human error) and vulnerability (e.g. system feature or functions) with arrows. This aids us to recognise and understand hidden relations. Some modification of the V^2 diagram methods has been made in order to adopt the research purpose. Johnson's diagrams have five legends; violation, event, continuation, contributory factor, and vulnerability. The author uses eight legends in this dissertation: system/artefact, operator, features/function, event/task, condition/emergency, vulnerability, violation/human error, and continuation/result (Table 5.7).

For the dataset of accident reports for applying the diagram method, 52 cases which have design issues in human error were chosen.

Table 5.7 Legends in diagram analysis

NAME OF LEGEND	LEGEND	EXPLANATION
System/ artefact		System or artefact associated with human errors
Operator		Operators (e.g. controllers, pilots) involved in case of failure of human–system interaction
Features/ functions		Features or functions that failed to comply with designed goals
Event/ task		Events or tasks that appear at the time of human–system interaction failure
Condition/ emergency		Special condition or emergency condition in which human operators failed to conduct correct functions
Vulnerability		Vulnerabilities of systems or artefacts for human–system interactions that may lead to human errors
Violation/ human error		Violation or human errors committed by operators
Continuation/ result		Connection from events or failures to next events or results

The analysis was qualitative and grounded. The process was, for each case, as follows:

(1) To develop a causal network that expressed the basic structure of events and influences described in the report.

(2) To identify a human–system interaction failure.

(3) To identify artefacts implicated in the failure. The artefacts failed contain organisational artefacts as well as physical artefacts.

(4) To express design concepts related to an artefact implicated in the failure in terms of the human–system interaction it coordinated. It means to find the expectation of designers of the system or artefacts. How did designers expect operators to use the system or artefacts designed in a particular manner?

(5) To identify the manner of the design-induced error that occurred in the way people in the system dealt with the situations and the artefacts. This was the most subjective step of the analysis, and none of the reports referred to design-induced error in any direct way. For example, in some cases the design-induced error appeared to be about distraction – about failure of short term memory in the operator when a system requested simultaneous tasks. A pilot, for example, seemed to be distracted about what to do now (the next procedure) while conducting urgent tasks. In other cases, design-induced error can appear in the form of "relying" – about finding ways of performing that would minimise a person's cognitive loads if stability of a system continued. A pilot, in one instance, seemed to make sense of what he should rely on in a system in a similar situation by finding a course of action that could be defended against exploitation of cognition. But this kind of inference was typically based on little direct evidence, so this part of our analysis remains highly theory-based.

(6) To describe the failure mode in terms of how this design of artefact undermined the coordinating function of human–system interaction resulting in design-induced error and ultimately contributed to the accident.

(7) To identify the influences of design implicated in the failure.

5.3.2 Results

Fifty two cases were examined and represented in diagrams. Short descriptions of the accidents, failed systems, and error modes are provided in the appendices. Figure 5.8 show an example of the diagram analysis.

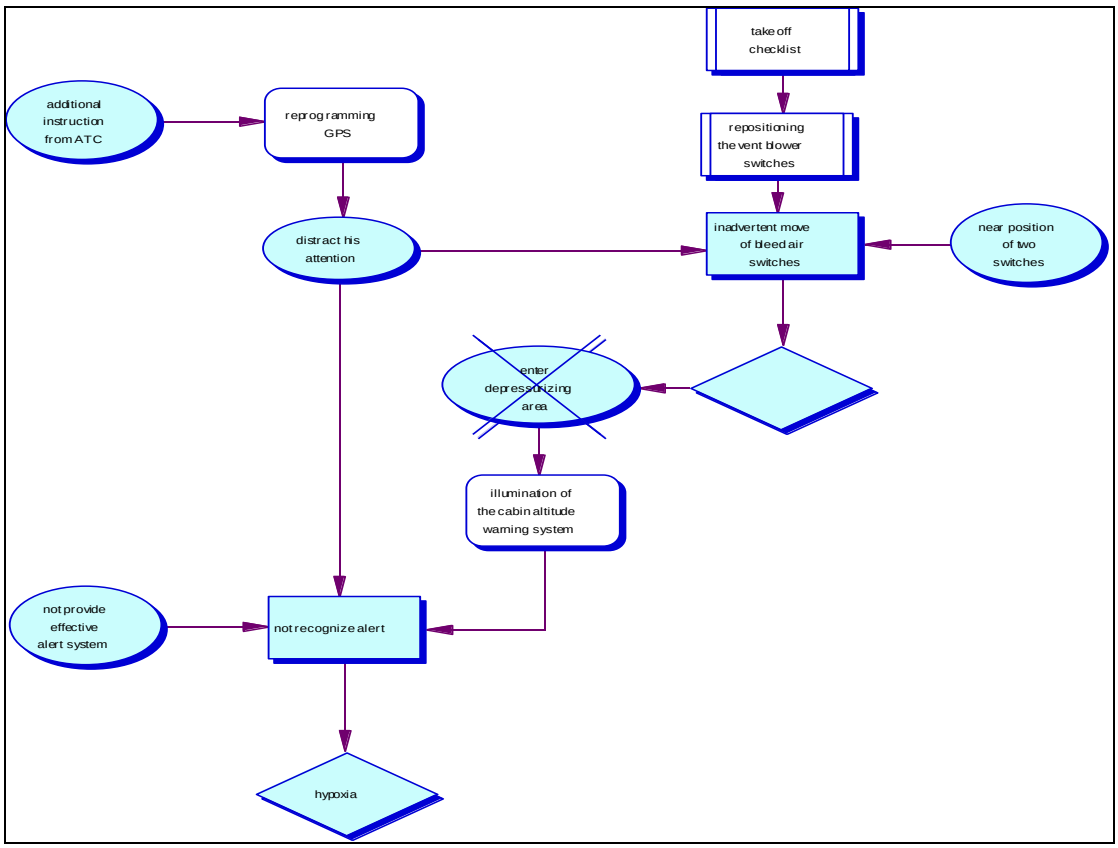


Figure 5.8 An example of diagram analysis (ATSB Occurrence number: 199902928)

ARTEFACT	COORDINATING DESIGN CONCEPTS
Takeoff check lists	All necessary itineraries could be included in the list that would be performed by operators without difficulty or error.
Operating of automatic level–up into a pressurising zone	Operators could recognise and respond to a critical state by continuously checking the current state of a system.
Alert systems	Operators could recognise warning signals provided by a system. The operator will look for alerts at any time or any circumstance.
FAILURE CASE	**FAILURE MODE IN TERMS OF DESIGN-INDUCED ERROR**
Incomplete takeoff check lists	Many items were included into an after take-off checklist procedure without considering the fact that a task, in case of failure or difficulty of the parts of jobs, delay or confound with other tasks. This led to puzzling of operators when they encounter an uncontrolled condition.
Unrecognised level-up into a pressurising zone	There were many itineraries to conduct on take-off check lists. If a pilot had to do one task in labour intensive cognition, this led to distracting operators' focus on continuously checking current altitude.
Misidentified location of a switch	Location of switches in similar shape but different functions plays an important role to the performance of operators. Many switches are similar shapes in close proximity. This led to unintended action while the operator was busy with other tasks.

5.3.3 Findings

Several expectations of designers towards both design of artefacts and operators were identified. The following are some of them:

- Trust in operation of many functions in a feature/procedure. For example, designers assume that the operator would operate without difficulties many functions in a feature or a procedure. The designers expect benefit of these designs would increase effectiveness or efficiency of a system / artefact and decrease product costs.
- Sensitivity of recognition of warning signals. Operators will perceive alerts without difficulty.
- Human ability to distinguish and to correctly manage devices located in close proximity can be decreased even in hectic conditions.
- Continuous monitoring tasks belong to human operators' responsibility in a procedure design.
- Changed design features which are different from previous designs in similar types of system could be coped with operators.
- Miscellaneous tasks such as data entry should not affect ability to conduct main tasks.
- An emergency check list could be listed without considering failure symptoms and achieved step by step from the first item to the final item.
- A generator failure could be easily found by operators because it causes an electricity cut. Therefore it is not necessary to prepare a specific check list for the failure.
- If design can put many functions into a system it will helpful for operators. It is not an important thing to consider how the operations of these functions would be different from the previous functions in operator's identification of the functions.
- A chart installed in a flight computer system. However, in the printing out it is difficult to identify characters in the printed chart.
- The responsibility to detect ice deposit in wings belongs to pilots. There is no need to provide a warning process.

- The operator could check a warning process before deleting data. There are many tasks, such as scanning runways, watching radar/computer screens, listening to radio for communication. It is easy to "click" a procedure; the operators have experience of lots of clicking manoeuvres.
- Automatic mode changes in computerised systems can increase flexibility of systems and utilise functions. Human operator can recognise these changes.
- Different designs of flight plans would be corrected by cross check by air traffic controllers.
- Limitations of systems would be well recognised by operators.
- After take-off, check lists could be achieved by pilots. The GPS configuration task would not distract the pilot's cognition.

Those expectations of designers, however, have failed during human-system interactions by different expectation of operators' on artefacts or systems. Followings are some examples of such failures.

- Many items were included into an after take-off checklist procedure without considering the fact that a task, in case of failure or difficulty of the parts of jobs, delays or confounds other tasks. This led to puzzling of operators when they encounter an uncontrolled condition.
- There were many itineraries to conduct on take-off check lists. If a pilot had to do one task in a labour intensive way. This led to distracting the operators' focus on continuously checking current altitude.
- An automatic warning system should have alerted operators to recognize a hazard. But operators being in a state of distracted cognition due to other tasks could not respond to a weak warning such as a light or a message in a screen display. This led to not recognizing the alert.
- The performance of the B737-400 series aircraft was superior to that of the B737-300 series aircraft. There was no effective process to check the different performance. That led to controllers considering that the aircraft were like types for the purposes of departure standard.
- The approach/departure controller elected to input data to the air traffic computer during the departure sequence. This was labour intensive and diverted his attention from the air situation display. This led to not monitoring the departure process of two aircraft.

- There is no alert system for a voltage failure, and the symptom of the failure looked like a display error. It might be a right decision that the voltage failure is not a cause of the warnings because cascade warning illuminations showed there was enough electricity in the system. That led the crew to overlooking the first item of the EFIS failure/disturbances checklist, which required a check of the generator voltage.
- The configuration of the Sector 3 console provided insufficient space to adequately display all relevant flight progress strips. As a result, controllers had developed the habit of removing strips at the earliest opportunity, thereby creating the potential for vital information to be missed.
- Computer based printed charts in a small size are difficult for pilots to read correctly. That led to misidentifying a correct taxiway.
- Without a clear prohibition standard, it is easy for humans to ignore unclear evidence and then consider as normal as routine practices. This led to misidentifying the ice deposit on wings.
- Without an alert, operators could not identify aerodynamic stall in advance.

Human errors related to design-induced error could be categorised as follows below.

- Distracting
- Puzzling
- Not recognise/ Lack of alert
- Differentiating from systems
- Autonomous performance in similarity cases
- Confusing with ambiguous condition
- Relying on a system in systems
- Routine tasks

Table 5.8 summarises design implications in human errors. Those error modes of design-induced error are categorised according to the most important issues that lead to cognitive failures of operators while operating a system. Each mode is explained in the table.

Table 5.8 Modes of design-induced error

MODE	EXPLANATION
Distracting	The operator should remember data in order to accomplish a job. Most data appearing in current tasks are stored in short term memory (SM) in human cognition. These data are easily distracted by simultaneous tasks because they are stored in SM. A subtask apart from a main task is also easily confounded by the main task. Design of tasks that require an operator to conduct two or more tasks simultaneously may cause distraction of operators. Such errors are termed *skill-based errors*.
Puzzling	The operator should interpret the situation and state of a system by examining external representations of the system. If a system does not give enough time and clues to identify and evaluate relevant logics of a system, logical errors may appear. Not enough representations also lead to such *rule-based errors*.
Not recognise/ Lack of alert	The degree of warning system should account for difficulties of tasks or safety degree of a system. If an operator does not have time to look around due to other tasks, the design of warning system not considering work environment degree would cause the operator not to notify the alert.
Differentiating from systems	If a system does not communicate continuously with human operators in the system by operating excluding the operators, the system would gradually deprive the operator dealing with the system of skill. Human operators, in such a condition, have differentiated from the system.
Autonomous performance in similarity	Various forms of similarity in design cause human errors. For many cases similar shapes, sounds or visual messages make operators commit errors because these tasks are conducted in skill-based performances.
Confusing with ambiguous condition	Ambiguity of procedures and operating methods that are not apparent to operators, create the possibility of other interpretations of the design methods such as procedure etc. in different ways.
Relying on a system in systems	The dependence on a reliable system is a human tendency. Automation and internal operations have increased the reliance on the system for operators. Without an effective communication system between operators and systems, an external or internal mode change would fail to attract the operator's focus or attention.
Routine tasks	Most jobs are routine tasks. Skill-based tasks save operator's cognition. If a system needs a task that is beyond routine procedure, the design of task should be such as to alert the human operator's cognition that has been adapted to a routine process.

5.3.4 Discussion

We have tried to identify human–system interaction and failures of the interactions. An analysis of accident reports followed. The kinds of design concepts implied in the failed interactions were examined. With the studies of literature reviews in Chapter 2 and accident report analysis in the previous section 5.2, design of human–system interactions may be categorised into five categories:

(1) Representation design: design for shape, location, or array of feature

(2) Alert design: design for operators to recognise an emergency state of a system

(3) Reliability design: design for a system itself sustaining the system

(4) Procedure or Rule design: design of procedures or rules in which operators conduct a function or accomplish a goal

(5) Communication design: design for an operator to communicate with other operators or systems

There are general assumptions by designers that limitations of design specification could be compensated by operators. Therefore expectations of design (designers) to operators play a vital role in the design-induced error process in the man–machine interaction process when operators have to get to grips with complex operational systems. If a design of a system just lets it operate automatically, not involving operators, this can lead to an error of operators who fail to notice a state of the system. People's compensation process often occurs in conditions where information is incomplete and ambiguous, and people necessarily fill in the gaps. In man–machine interaction, operators resort to various practices to achieve this. The practices are results of operators having gained experience. Operators have continuously analysed and tried to interpret the symptom of conditions in a system. Those analysing processes are to investigate the underlying meanings of the design of a system. Many evidences show operators' misunderstandings of what are the purposes of design because in their previous experiences the assumption of design was correct.

The compensation process is a dichotomy: trust or distrust. If an operator has good experience in similar conditions, she (he) believes representations of a system actually so as not to pursue further investigation of other evidences. Development of false assumptions of human operators on system operation is a causal factor of design-induced error.

Who is responsible for these errors? It is not easy to answer the question. But the

concept of design-induced error suggests that not only operators but also designers should consider contributory factors of their design to errors.

Table 5.9 Design Categories of human–system interactions

DESIGNS	ERROR-INDUCING DESIGN CONCEPTS IMPLIED BY DESIGNERS
Representation design	Similarities of positions, array, colour, shapes of artefacts make it difficult to distinguish one artefact from other artefacts.
Alert design	When a system continues a procedure which could go into an emergency state if people fail to do proactive action before entering the state, no or a weak alert system that could alert people who were in a state of focusing on other tasks.
Reliability design	Automatic compensation or control system that could not communicate with people or not show the state of system.
Procedure design	Complicated procedures or a procedure that is not prepared for failing, conducting a previous procedure or delay of the procedure.
Rule design	Rules that clearly approve or prohibit a procedure or committing of a task
Communication design	Congested communication, difficulty of communication or ineffective checking system for communication

Error-inducing design

These issues above may not be well conceived by designers due to the unreasonable nature of these events for the designers. Designers consider well-defined procedures in accordance with logical operations of a system. Their mathematical and mechanical logic, however, could fail in human–system interaction operations if they did not prepare and consider the fact that the mind and behaviour of human operators, who interact with artefacts, would be affected by the design. It is important to consider a margin in human–system interactions like safety factors.

Error-inducing design refers to the design of a system that does not provide operators with proper knowledge to overcome a stereotypic procedure, or assumes that operators would act correctly or respond exactly to the demands of a system at the time of hectic operation circumstances, which leads to the operators making errors.

There are two main patterns of error-inducing design. The first involves designs that do not provide people with proper knowledge to overcome a stereotypical procedure. They

are the *misusages of design*. Design has some functions to provide information to operators. However people in the system would be misled by the information, if presentations of the information are not relevant for human operators to identify or evaluate a state of systems, particularly in temporal decision making conditions, and the representation has been used in different ways. The system only provides superficial information for operators, even if not for designers.

For example, when an emergency procedure is slightly different from a previous design of the procedure due to technical changes, operators can easily fail in the new procedure in certain circumstances. Human operators have accumulated habit in the procedure. The emergency procedure would be operated in hectic conditions. As a result, the operators follow the previous procedure unconsciously.

Features and functions of systems also can be involved in failures in human–system interactions. For example, design concepts and rules that simplified a continuously variable world into straightforward and abstract forms (e.g. a red sign means stop) or representations (such as array, colour, shapes, and procedures) which support a natural kind of understanding, by which people understand the functions of a system in order to make their problems tractable.

However, there will be some situations in which their agreements are not clear or one part of them changes the rule of design. For example, a change in an array of switches in a display panel may confuse operators who manage the system, if the change was not fully realised by the operator. And at the time of unfavourable circumstances these will present much higher risks. In a system like an aircraft, which is complicated in degree, large in scale, even a moderate difference of some design rules will mean that operators in the system can easily fail to understand correctly the changes within fairly short time-spans and many operations. Thus consistent manners in both the design rules and operator's understanding provide adequate protection of system operations. It is a problem of understanding in tasks or functions of a system.

The second pattern is *design omission*. Designers, in this case, miss designing functions or features in a system because they think the design is not necessary, taking it for granted that it belongs to operators' cognition. For example, in one case a pilot had forgotten to conduct a compensation task for a depressurising condition, recognition of his or her memory failure would be difficult because the pilot have other tasks to conduct and the aircraft will level up automatically above the maximum altitude of depressurisation. Automatic mode change would not be noticed without an effective alert system design. Missing the design could lead to failure of whole procedures. Although the system might have an artefact (e.g. an indicator showing height of

altitude) that was meant to detect the state of a system, the system relied on the operator's noticing, and being prepared to take action. It required of the operator continuous and strong consciousness for the task, for some aspect of a state of system that indicated the aircraft had passed over the limitation of permitted altitude.

In the course of human–system interactions, the operator's recognition remains in an assurance of system reliability and does not make an effort to detect unexpected consequences of the operations. It means that in the absence of effective stimulants to indication of a state of a system, people assume that there had been none to involve to the system. Research has shown that this is a natural default decision of humans [Busby and Hibberd, 2004]. Findings point out that whether it is a time for an operator to involve in a system activities are highly cognitive demanding tasks, which need to continuously explore a state of a system. Therefore, in such a system human operator's cognition is exploited. It makes the protection of a system vulnerable and the system's goals ineffective. It is a problem of how to provide relevant means to improve recognition or perception of operators on the state of a system.

As a conclusion of this case study, effective design must consider that safety of a system needs necessary coordination between designers' understanding of operators' cognition and performances, and operators' perspectives of a system. Designers should identify potentially misused designs and design omission. It may be subtle and difficult to identify such problems. Since operators can never perform in a mechanically logical manner for all circumstances, design must provide the operator of effective means for human-system interactions. It also must be consistent with the experiences of operators and intended functions, otherwise human operators undermine designed functioning. It may be important that design should improve flexibility and creativity of human operators.

5.4 Summary and limitation of the analysis

5.4.1 Summary

The case studies revealed two things that make sense. Firstly, there are many cases of human errors in human–system interactions. As many human error researchers have suggested, such errors could not be prevented or negated only by the efforts of human operators. The design of systems should contribute in order to overcome these failures. Secondly, it is hard to identify relationships between design and human errors. Many accident reports could not comment on reasons for errors. Such difficulties stem from inherent limitations of investigation into human errors. People involved in an accident may find it difficult to explain why they failed because they may reason that the failures are psychological effects or symptoms.

Table 5.10 Summary of case study results

RESEARCH QUESTIONS	RESULTS	CROSS REFERENCE
What is nature of human error? How human error cases could be found in accident reports? Etc.	Human–system interaction failures were found in more than 40% of all accidents. Human error types, factors leading to errors, and meta-theory were also examined.	Section 5.1
In which artefacts or systems do human operators make errors frequently?	Ten systems themes were grouped and examined in detail by marking up on the document. Human–system failures cases are found in various artefacts or systems including automated systems.	Section 5.2
Is there any way to represent relationships between design and human error?	A diagram representation method is proposed. The diagram analysis which shows relationships of design and human errors in diagrammatic form was developed and conducted in 50 cases.	Section 5.3
How can the meta-theory of design-induced error help to identify mechanisms of errors and implicated design concepts that affect human operators?	There were not many examples of clear description of relationship between design and human error. Without meta-theory most cases may be interpreted as just human errors. Theories provide a possibility to recognise their relations.	Section 5.2

Furthermore, if human operators who were involved an accident are dead, they are not able to reveal the reasons for any errors. Hence, the meta-theory and the diagram analysis are proposed to help people, including designers, to recognise relationships between design and human error. Table 5.10 summarises results of the case study.

5.4.2 Limitation of the case study

It is inevitable that there are possible biases and limitations for the case study. This research, analysis of relationships between design and human error, is focused on qualitative analysis rather than quantitative analysis in methods. In order to prevent misunderstanding of results of the study, it is important to present limitations of the case study, of which the author was aware during research.

Generalisation issues

This study may not be generalised for two reasons; limitation of a dataset and area of cases. If this study was to be generally applied to other fields or industries, the dataset should be gathered from various accident databases. The study used 562 cases from the Australian aviation accident report system. The more data that can be gathered, the more the research can generalise the result of case studies. However, the result of the case study may utilise a prototype study by which research can develop experimental sets for more extensive studies.

For contextual limitation, the case study focused on the aviation system. There may be some deviation to other industries for example if the case study was conducted in the chemical industry, manufacturing or health care etc. The findings of this case study may be more applicable to the sophisticated domains, such as nuclear power plants that adopt highly automated systems.

Validity of the analysis

The analysis was conducted by the author. Therefore, the result of the case study is very subjective. However, many human error researchers have used same technique of subjective analysis, because analysis of human errors needs human interpretation on a case. Therefore, precise statistical results are not of much importance for this research.

According to an issue with the evaluation methods, the following steps were taken to identify design-induced error cases.

- Identify human errors
- Identify systems that interact with humans
- Identify modification of the system after the failure.

As recommendations in accident reports touch many items, it is difficult to connect the relationship between design and human error. The reports comment on various items to prevent such errors recurring, including training, and emphasise operators' attention to following procedures. Therefore, it is necessary to develop methods by which people can find specific relations in various expressions.

Even this method is not fully matured, it could help to find design vulnerabilities to human–system interactions.

According to an issue with the diagram representation, the diagram method is not fully tested. It is a prototype method which needs further development and evaluation.

Chapter 6. Knowledge Acquisition and Sharing Methodologies

Previous chapters discussed design issues related to human–system interaction failures, and then developed a meta-theory of design-induced error by adopting meta-theoretical assumptions. As a practical approach to the concept developed, the remaining chapters will investigate ways the developed theory can assist designers as well as people (e.g. accident analysts) who want to recognise design issues in human−system interaction failures. The research particularly concerns knowledge-management systems that are an emerging area of the field of knowledge acquisition and sharing, in future as well as currently. The application of the methodology focused on developing an ontology and on accident reports that contain the concept of design-induced error.

This chapter briefly reviews knowledge-management techniques, knowledge acquisition techniques, knowledge modelling, and knowledge organisation structure (i.e. ontology), and their benefits. This chapter also reviews the ways the field of engineering design has used ontologies and how ontologies would help designers in this case of research (e.g. accident analysis).

6.1 Problems in knowledge sharing of human error

The meta-theory of design-induced error has argued that the different perspectives between designers and operators should be considered as a main causation of design-induced error theories. From this assumption an important way to bridge the gap between them is to share the knowledge addressed in theories. If designers had a chance to understand operators' perceptions on the design of a system, the design could be assisted with possibilities of human–system interaction failures identified, and a more cooperative system designed. If we agree this notion, there is a question to help designers: How to share the knowledge of design-induced error?

Psychological knowledge that explains phenomena of human behaviour is important information for designers and system developers, especially those who design highly

critical systems (e.g. aviation, nuclear power plants). One finding has suggested that human errors are attributed to many aviation accidents [NASA, 2002] and many other human error studies have produced similar results. However, it is one of the difficult areas to capture useful knowledge from research in order for it to be used in the design process.

Accident reports which are very standardised and therefore most likely to be amenable to automation, contain a number of items of information that can be used by designers to understand the effect of their design on human behaviours. A number of accident reports have being generated in many countries by those who have responsibility for investigating accidents and recommending safety issues including design issues of systems. The use of accident reports in order to understand the role of design in minimising those human errors is therefore an invaluable resource.

However, since accident reports exist in the form of unstructured texts, it is difficult to extract specific knowledge from the unstructured documents systematically (or automatically) for use in a knowledge-based system due to ambiguity and the diversity of expressions of related concepts. Additionally, as reports may describe a number of factors that contribute to an accident, the reader may easily lose his/her focus and be confused by the amount of information [Johnson, 2000].

Therefore it will be useful for designers, in order to understand the knowledge interpreted from a particular point of view (e.g. in this thesis a meta-theoretical point of view of design-induced error), if we can develop a methodology that can identify concepts and their relations related to the point of view in a collection of accident reports in an effective way. It is also helpful for use of the information contained in the accident report in computer-based systems (e.g. the Web) if the accident reports are transformed into easily accessible formats.

There have been many attempts to improve the accessibility of the accident report systems. Most of them have focused on developing database systems (e.g. National Transportation Safety Board (NTSB) Accident Database & Synopses, USA). However, knowledge that can be extracted from database systems is limited by their structures and formats. When we construct a database system, parts of the knowledge contained in an original document may therefore inherently be lost.

Now, the obstacle to sharing the knowledge of human-error theories with designers is how designers can gain the information and knowledge more effectively and easily than before. The aim of this research was therefore to examine and demonstrate the possibility of capturing psychological concepts (i.e. design-induced error) from

documents and representing their relations in an effective form (e.g. a graph, a network) by developing an ontology that formalises related concepts of error and design which match psychological human error theories.

6.2 Knowledge, knowledge management, and knowledge acquisition

"Knowledge management", the capture of knowledge for further reuse, is one of the prevalent technologies taken up by industry in recent years [McElroy, 2003]. Many researchers have argued that managing knowledge is the best practice in current organisational management [e.g. Davenport and Prusak, 1998; Nonaka and Takeuchi, 1995]. Techniques of knowledge management (KM) have been developed for capturing knowledge that could be easily lost without intensive, deliberate effort [Wielinga et al., 1997]. Techniques of KM are divided into two broad categories: knowledge acquisition/extraction and knowledge modelling [Schreiber et al., 2000; Preece et al., 2001].

Milton et al. [1999, pp.620] summarised five key KM activities as the following:

"Personalisation is the activity of sharing knowledge mainly through person-to-person contacts. This can be facilitated by investment in current IT systems [Hansen, Nohria and Tierney, 1999]. There is also an opportunity for knowledge technology to enhance this process by providing tools to allow employees to communicate more effectively, e.g. by ensuring they are clear in their terminology and the ways in which they conceptualise a domain.

Codification is the activity of capturing existing knowledge and placing this in repositories in a structured manner. This is the most likely area where a knowledge technology based on knowledge acquisition techniques might be applied, the aim being to make the process more efficient, for instance by using generic models, and more effective, by using a range of specialised techniques.

Discovery is the activity of searching and retrieving knowledge from repositories and databases, such as using intranet and internet systems. There is potential here for knowledge technology to aid in search procedures such as automatic construction of ontologies.

Creating/ innovation is the activity of generating new knowledge, vital if an

organisation is to remain competitive [Nonaka and Takeuchi, 1995]. Present technologies have fallen short of providing any significant impact on knowledge creation [Bond and Otterson, 1998], and there seems little doubt that in the foreseeable future this is likely to remain a primarily human endeavour. There is, however, an opportunity for knowledge technology to be of assistance if only in providing sophisticated brainstorming tools.

Capture/ monitor is the activity of capturing knowledge as people carry on their normal tasks such as interacting with people and computer systems. This is an attractive notion, as it does not have the overhead of taking people off-line in order to capture their knowledge. One promising opportunity is to provide knowledge tools that both aid people in their activities and in so doing capture important knowledge, such as providing an audit trail of decision making."

6.2.1 What is knowledge?

In knowledge management, data, information and knowledge are distinguished. However, there are many ways to define these concepts. In many definitions of the concepts, "data" is in general considered as a raw source. "Information" is structured data, in which we can gain knowledge from the information in a certain context. However, it is difficult to make a decision only with information because information is not clearly associated with contexts. "Knowledge" is information associated with contexts. For example, when we see traffic signs we understand the meaning of signs and activate our action according to our knowledge of signals. "Red", "green", "stop", and "go" are data. "Red sign is to stop" and "green sign is to go" is information. The knowledge is that we know which sign we have to follow when we see the sign because the meaning can be changed according to our position, such as a pedestrian or a driver.

Knowledge is considered harder to detect than information because it is a kind of beliefs and commitment [McMahon et al. 2004]. A question of "what is knowledge" is a difficult question to answer because that is in a human's head. For example, knowledge of driving a car is something one has in his/her head. Therefore knowledge is ability, experience, information, or aptitude etc. of our own. Knowledge can be divided into two kinds: declarative knowledge and procedural knowledge. Declarative knowledge is what we know (e.g. the laws of motion, the structure of DNA). On the other hand, procedural knowledge is the way we know how to do things (e.g. driving a car, boiling an egg).

The other ways to categorise knowledge have been discussed in many research studies. The most famous categorisation in KM may be explicit knowledge and tacit knowledge

[Nonaka and Takeuchi, 1995]. There are various explanations about tacit knowledge (Table 6.1). Tacit knowledge [Polanyi, 1966] may be a kind of reflection of experience. It is essential for expert performance, and experts often do not know they use tacit knowledge. As a result, experts find it very difficult to describe their tacit knowledge. However, it is essential to capture and share with others. The task of knowledge engineering in KM is to transfer tacit knowledge to explicit knowledge in various ways.

EXAMPLE	SOURCE
legal expertise – determining critical case factors; identifying precedents; developing analogies; building an argument	Marchant & Robinson 1999
knowing how to handle face to face selling; how to maximise high probability sales situations; salesmen's rules of thumb	Wagner et. al. 1999
setting up a scientific experiment – e.g. the care taken in clamping the apparatus; in preparing experimental materials (polishing a metal suspension thread; greasing a silk suspension thread)	Collins 2001a
riding a bicycle; dancing	Collins 2001b; Cook and Brown 1999
applying social rules; following conventions	Collins 2001b; Janik 1988
speaking acceptable phrases	Collins 2001a
"knowledge ... manifested in traditions"	Collins 2001b; 1974
nurses intuitions about patients' conditions	Herbig et. al. 2001; Josefson 1988; Leonard & Sensiper 1998
managing oneself (knowledge about the importance of tasks), and managing others (how to assign tasks)	Wagner & Sternberg 1986
deciding which journal to submit an article to	Wagner & Sternberg 1986
drawing inferences from various news stories	Baumard 1999
doctors' rules of thumb for psychosocial problems	Andre et. al. 2002
making, and playing, musical instruments	Cook and Brown 1999
baker's ability to make tasty bread	Nonaka & Takeuchi 1995

Table 6.1 Examples of tacit knowledge (Gourlay, 2004)

Type, source and context are main considerations used in knowledge management to characterise information [Court, 1995; Bouthillier and Shearer, 2002]. Which type of information or knowledge we have to develop is an important element for knowledge

management research. It means what kind of information is required to undertake a particular task. For an accident report analysis, we need a particular structure for the classification of information (this was a consideration of developing an ontology of design-induced error).

The source of information and knowledge is where we have to seek the information and knowledge. Experts, documents, or data are main sources of knowledge extraction. For this research, accident report documents were adopted as a knowledge source. To provide reliable information and knowledge they need some criteria such as availability, accessibility, applicability, authenticity and amount [Turner, 1977]. Accident reports are created by investigators who mainly come from a governmental body (e.g. Air Accidents Investigation Branch (AAIB) of the Department of Transport for aviation accident investigation in the UK). These days they provide accident reports in the form of pdf or html files on websites. Although it is possible to access such documents readily, there are still issues of identifying relevant knowledge from the documents.

From which context we are to try to acquire information and use knowledge is important. Accident reports are produced by investigators who follow documentary reporting rules. They want to include as much information as possible because the reports may be used by persons from a number of fields such as regulators, psychological researchers, and designers. As a result, the reports contain a range of information on matters such as personnel who were involved in the accident, system or artefact (e.g. aeroplane), external factors (e.g. meteorological information), medical, and technical analysis (e.g. fire or explosion).

6.2.2 Making tacit knowledge explicit

The main quality of knowledge is what the knowledge pertains to, and how to represent the knowledge. While knowledge exists in two ways: formal (i.e. explicit) and informal (i.e. implicit or tacit), knowledge creation in organisations is flourishing when tacit knowledge is mobilised and converted into explicit knowledge [Nonaka and Takeuchi, 1995]. However, owing to its unstructured and uncodified forms, implicit knowledge and tacit knowledge cannot be easily shared between designers [McMahon et al., 2004]. Making tacit knowledge to explicit knowledge is an important issue in knowledge management systems and AI (Artificial Intelligence) fields.

The development of knowledge management techniques with research on psychology give now a room for a possible way to understand tacit knowledge (e.g. in this thesis,

design-induced error) and turn this knowledge into a reusable form. In order to make it possible, knowledge exploitation processes have been suggested [Milton et al., 1999]. This process in general begins with a knowledge elicitation process, and ends in a knowledge modelling process (Figure 6.1).

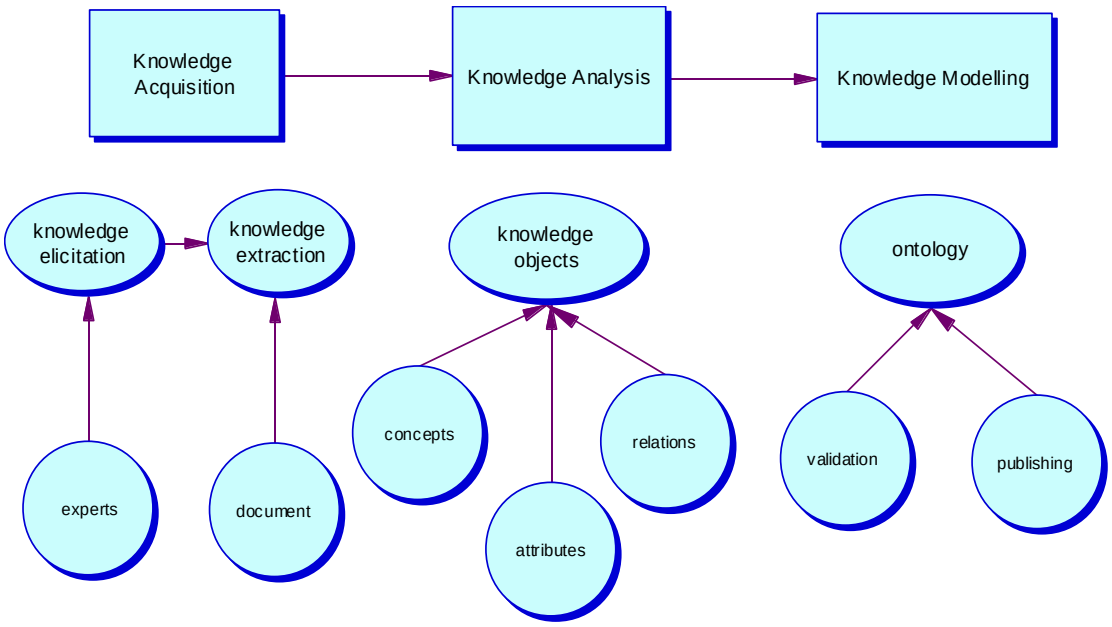


Figure 6.1 A knowledge modelling process (from Milton et al., 1999)

We can conceptualise our knowledge in terms of knowledge objects. Knowledge objects are concepts, relationships between objects, and properties of the objects (i.e. attributes and values). It is important when capturing knowledge to break down (analyse) knowledge into conceptual "nuggets" (i.e. knowledge objects), and present these 'nuggets in clear ways to validate, extend and communicate the knowledge [Milton et al., 1999].

Concepts, core of knowledge objects, are things that constitute a domain. Physical entities (e.g. products, components, machines), information (e.g. ideas, plans, goals), information sources (e.g. documents, databases), people and organisations (e.g. roles, groups), domains and techniques (e.g. physics), functions (i.e. purpose of objects or roles), issues (e.g. problems and solutions, pros or cons), phenomena (e.g. physical mechanisms), other behaviour or constraints etc.

Attributes are the qualities or features belonging to a class of concepts. For example, physical objects have a weight, a shape and an age. Jet engines have a weight, a thrust and noise level. Ideas have a source, a format and an importance. Organisations have a number of employees, a turnover and a product range.

Values are the specific properties of a particular concept such as its actual weight, age,

and format. There are two types of values: numerical (e.g. 10 years old, 100kg) and adjectival (heavy, young) values. Each value is associated with a particular attribute. For example, the value 120℃ applies to the attribute of temperature. Only one value can be associated with a particular concept. For example, the colour of a car cannot be associated with both blue and red.

Relationships are the way concepts or other knowledge objects are related to one another. The most important relationships are "is a" relation that shows classification (e.g. car is a vehicle) and "part of" relation that shows composition (e.g. a wheel is part of a car). Relationships can be related to a value (e.g. an elephant is heavier than a mouse). Relationships usually are represented as labelled arrows in a diagram.

6.2.3 Knowledge acquisition techniques

Knowledge acquisition involves the activities of knowledge eliciting, data analysis and domain conceptualisation [Scott et al., 1991]. Aims of knowledge acquisition are: (1) to capture or elicit knowledge (mainly from experts) as efficiently as possible, (2) to structure knowledge, (3) to validate (check) the knowledge is correct, relevant, best practice and useful, (4) to publish knowledge in a form that can be used for end-user documentation (e.g. web pages) or software implementation (e.g. design specification) [Milton et al., 1999]. In order to develop an ontology of design-induced error, we need to know how to capture the underlying meanings and then how to conceptualise the meanings captured. Figure 6.2 shows a general framework of knowledge acquisition (KA) from various knowledge sources (Selbig, 1986, in Wagner, 1990).

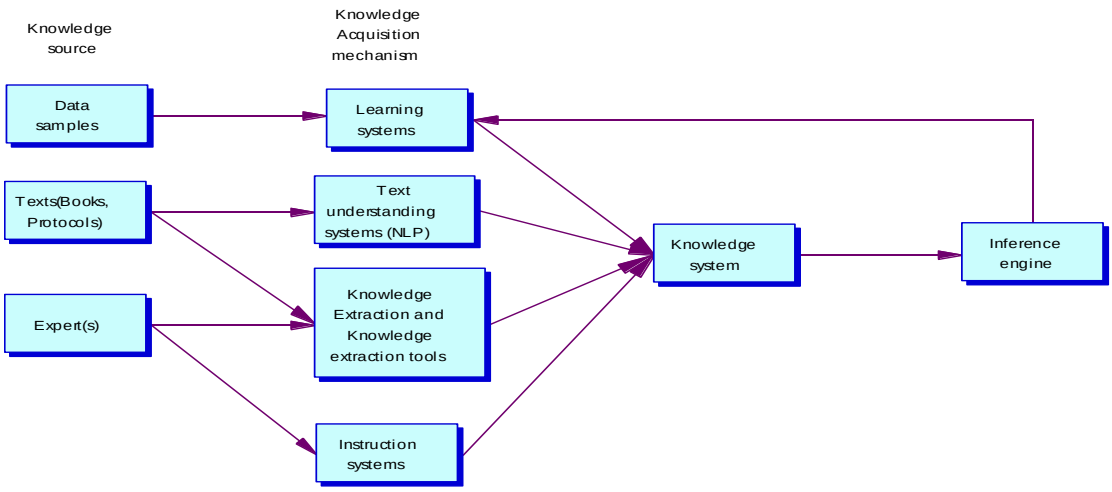


Figure 6.2 Descriptive KA Framework (adapted from Selbig, 1986 in Wagner, 1990)

Knowledge acquisition needs a knowledge elicitation methodology from experts [Hoffman et al., 1995]. Milton et al. [1999] proposed general steps for knowledge acquisition as follows:

1. Conduct an initial interview with the expert to (a) find the scope of what knowledge should be acquired, (b) determine to what purpose the knowledge should be put, (c) gain some understanding of key terminology, and (d) build a rapport with the expert. This interview (as with all encounters with experts) should be recorded on either audiotape or videotape for later analysis.

2. Transcribe the initial interview and analyse the resulting document (called a "protocol") to produce a set of questions that cover the essential issues across the domain and that serve the goals of the knowledge acquisition exercise.

3. Conduct a second interview with the expert using the pre-prepared questions to provide structure and focus. (This is called a "semi-structured interview".)

4. Transcribe the semi-structured interview and analyse the resulting protocol, looking for knowledge types: concepts, attributes, values, classes of concepts, relationships between concepts, tasks and rules.

5. Represent these knowledge elements in a number of formats, for example, hierarchies of classes (taxonomies), hierarchies of constitutional elements, grids of concepts and attributes, diagrams, and flow charts. In addition, document, in a structured manner, anecdotes ("war stories") and explanations that the expert gives.

6. Use the resulting representations and structured documentation with contrived techniques to allow the expert to modify and expand on the knowledge you have already captured.

7. Repeat the analysis, representation-building and acquisition sessions until the expert is happy that the goals of the project have been realised.

8. Validate the knowledge acquired with other experts, and make modifications where necessary.

The above steps constitute knowledge acquisition activities (Table 6.2). Knowledge engineering techniques have been developed to assist such processes and activities.

Knowledge acquisition techniques are divided according to information formats and types. When information is captured we need to extract useful meanings from the information. For the knowledge acquisition approach we have to decide preliminary knowledge sources (e.g. experts, expert-domain map, end users, documentation). Then we need to validate the captured knowledge, e.g. validation plan, validation resources (commitment from expert). Knowledge analysis consists of the tool/method of analysis, knowledge objects, and quality of transcript analysis.

PHASE	STEPS	ACTIVITIES
Planning	Understand the domain	Learn terminologies, concepts, and problem-solving strategies
	Identify domain experts and users	Identify primary experts and users
	Define the problem scope	Meet with experts, users, and managers to define the problem
	Identify the type of application	Investigate problem characteristics and identify the type of applications
	Develop process models	Perform task analysis and identify key processes
	Plan KA sessions	Develop session agenda
Extraction	Explain KA approach	Introduce KA concepts and methods to experts
	Discuss objectives of KA sessions	Explain objectives and procedures of KA sessions
	Conduct KA sessions	Employ KA techniques to acquire knowledge
	Debrief experts	Conclude KA sessions
Analysis	Analyse KA session outputs	Identify concepts, objects, or entities Identify attributes associated with each concept, object, or attribute Identify possible values of attributes Identify class-instance, part-subpart relationships Identify heuristic rules
	Transfer knowledge into representation	Use diagrams to represent knowledge structures Transfer object-attribute relationships into rules Transfer part-subpart relationship into rules
Verification	Develop test scenarios	Create test scenarios Collect problem scenarios from experts and users
	Verify knowledge with experts	Verify knowledge structures and rules

Table 6.2 Summary of steps and activities of a knowledge acquisition methodology (adapted from Liou, 1990)

Between knowledge capture (extraction) and knowledge modelling, knowledge analysis is necessary (Milton et al., 1999). Knowledge analysis begins with identifying key knowledge from a text document, and then selecting the appropriate types of knowledge (e.g. concepts, properties, problems). Highlighting text using coloured

highlighter pens often performs in this process. An ontology should be developed during the early stages of analysis in order to identify what main types of knowledge objects are there, how these knowledge objects are related to one another, and how the knowledge will be presented using knowledge models.

Transcript analysis involves analysing a transcript or other document to identify the relevant knowledge. The analysis must be driven by the aims and requirements of the project. Therefore, the analysis plan should be developed before analysis begins: what sizes and types of knowledge to pick out, how to model the knowledge.

To plan knowledge acquisition we have questions such as which domain, how much data and how to capture the knowledge? **Table 6.3** briefly presents various techniques and technologies of capturing and analysis of information and knowledge. Such technologies have recently been developed and are still under development.

There are two criteria to find the areas of knowledge that will provide the best business benefits. First, we have to consider the importance for customers: how important is the knowledge for the end-user? Second, how easy is it to capture and deliver the knowledge to the end-user? For capturing knowledge we have to breakdown the categories of the knowledge into useful forms with relevant criteria.

FORMAT AND TYPE OF KNOWLEDGE		CAPTURE TECHNOLOGIES	TECHNOLOGIES FOR THE EXTRACTION OF MEANING
Textual	Structured	Paper/ electronic format Handwriting recognition (Tablet PC, digital pen) Electronic notebooks (MECE, PENS, EEN, NMR)	Knowledge acquisition techniques. PC PACK IBM Intelligent Miner for Text: provides a suite of text analysis and text search tools. Knowledge modelling techniques. Knowledge engineering methods: EboK, MOKA, PICK, CORMA, XPERTS, CommonKADS.
	Unstructured	Paper/ Electronic format. Handwriting recognition (Tablet PC, digital pen) Electronic notebooks (MECE, PENS, EEN, NMR) Liveboard/Tivoli: interactive whiteboard application for group meetings.	InBASED: Intranet Based System for Engineering Design, prototype for improving communication in product development project by using visualised project data. Design rationale system
Verbal	Structured	Audio/Video equipment. Manual transcriber: a software tool for manually transcribing recorded audio into text has been developed. Speech recognition software: navigation systems, used mainly for telephony applications with a restricted vocabulary.	Speech recognition: multimedia indexing applications, spoken document retrieval through text query input. Audio notebook: when used to take notes from a structured discourse. WASABI project: applies a variety of applications to a transcript of a live broadcast to identify information elements, to generate queries and extract relevant data to the ongoing discourse. Rough'n Ready: an identical goal to WASABI but analysis is done offline.
	Unstructured	Audio/Video equipment. Manual trascriber: a software tool for manually transcribing recorded audio into text has been developed. Speech recognition software: speech into text software (Via Voice, Dragon Speech)	SpeechSkimmer: a system for interactively skimming recorded speech. W3: making and using near synchronous, pre-narrative video. Audio notebook: when used to take notes from a meeting. MeetingMiner project: text transcripts from speech recognition software are analysed and prompt questions during meetings.
Pictorial	Structured	CAD software: capture standard engineering drawings.	Space Pen: enables designers to make annotations on virtual 3D models, generating web-based pages. CAD/CAM links: knowledge from CAD model is transferred to CNC machines.
	Unstructured	Liveboard/ Tivoli: interactive whiteboard application for group meetings. Tablet PC to capture sketching?	W3: making and using near synchronous, pre-narrative video. Audio notebook: when used to create sketches during a meeting. sKEA project: sketching knowledge entry associate, a system designed for knowledge capture via sketching.

Table 6.3. Technologies that can be used for knowledge capture and extraction (Huet, 2004)

6.3 Knowledge modelling and knowledge organisation structures

Knowledge acquisition is not useful if the knowledge cannot be shared with other persons (e.g. designers) and reused. Therefore, knowledge modelling is important for constructing a knowledge-based system that facilitates reuse of the knowledge. The development of knowledge organisation structures (KOS), such as classifications and ontologies, is at the core of knowledge modelling process. There are many knowledge modelling techniques such as "CommonKADS" [Schreiber et al., 1999], "Protégé 2000", or Multi-perspective modelling [Abdullah et al., 2002; Gennari et al., 2002].

The term "model" refers to any structured knowledge that reflects the world of interest (i.e. a system). It helps us to make sense of the world. We can use a model to capture essential features of a system. Models exist both internally as 'mental models' and externally as "cognitive artefacts". Cognitive artefacts can take many forms: written texts, graphs, diagrams, pictures, equations, computer-simulations, etc. While these different kinds of models vary greatly in their form and function, they all share certain desirable properties. Creating a model can be achieved by breaking a system down into more manageable parts that are easy to understand and to manipulate.

Knowledge modelling involves constructing a structured representation (e.g. diagrams, grids, hypertext) of knowledge objects. Knowledge models can help users to think clearly, be organised and be analytical. These also help to validate the knowledge with experts. It can be possible to communicate, to use and re-use the knowledge with the developed knowledge model.

A knowledge model should be clear and unambiguous [Abdullah et al., 2002]. It should not be too small or too big. Most of all it should provide a particular perspective of the knowledge. There are important types of knowledge models: network diagrams, various types of matrix (grid, table), and annotation. Network diagrams comprise nodes and links. Nodes are shapes with associated text and they represent knowledge objects. Links are lines or arrows (sometimes labelled) and represent relationships. Hierarchical forms of networks are represented in the style of a tree. Maps can be used for non-hierarchical forms of network diagrams. Matrices are two-dimensional grids with filled-in grid cells. There are two main types of matrix: attribute matrix and relationship matrix. An attribute matrix is concepts *versus* properties (values). A relationship matrix is used for problems *versus* solutions or processes *versus* resources. Cell entries can be

symbolised by a symbol (e.g. ticks, crosses, question marks), colour, number, or text.

Annotation pages are a collection of pages detailing the knowledge in the domain. They consist of one page per relevant knowledge object. Annotation pages use structured text, diagrams and pictures. Annotation pages summarise all relevant knowledge and form the basis for the content of web pages. Annotation pages should use generic headings to clarify and aid description. Generic headings are sets of headings applying to a class of knowledge objects. They provide an annotation page that is a form to be filled-in. The structure of annotation pages is a special form of frame. It provides a checklist for knowledge capture, and helps clarify what has and has not been captured.

An ontology, a kind of knowledge model, is a "formal description of the entities within a given domain: the properties they possess, the relationships they participate in, the constraints they are subject to, and the patterns of behaviour they exhibit" [Uschold and Gruninger, 1996]. Ontology provides detailed entity and relationship definitions that go beyond anything provided by reference models.

6.3.1 What is ontology in knowledge engineering?

As mentioned in Chapter 3, the term ontology has two meanings philosophically and knowledge technically. For knowledge management researchers, ontology is a model or definition of a world interest.

Ontology is one of the important parts of knowledge management systems (KMS) that have been identified as one of the key technologies in current and future engineering design [Guarino, 1998; Abar et al., 2004]. The ontology has been used for the basis of exploitation and use of accumulated knowledge because an ontology is a classification structure.

KMS technologies have improved communication between human and machine as well as between human and human. How to create and share knowledge in communities is a key challenge to knowledge management (KM). In order to organise and share knowledge in KMS it is necessary that domain knowledge should be transformed into machine accessible and applicable forms and structures. Such tasks are called "codification of knowledge" [McMahon, 2002]. Codification is a methodology to collect and organise knowledge that can be used and shared in KMS. However the difficulty of organising knowledge partly stems from knowledge itself, i.e. its terminology and relationship. Knowledge, unlike information, is regarded as a deeper understanding of a fact. It represents a belief in a fact associated with actions and

processes of information [McMahon, 2002]. Knowledge has a diversity of expression of a phenomenon (e.g. terminological diversity). Ontology provides a solution to tackle such a problem.

Knowledge consists of concepts and their relations in knowledge-based systems. An ontology is a hierarchical basis to codify concepts and relations with hierarchical structures and mapping a natural language in text with ontology in KMS because ontology is defined as an explicit specification of a conceptualisation [Gruber, 1993]. The term "concept" can be defined as "a collection of propositions about a separable component of the world and is designated by a label" [Darlington, 2002]. Relation refers to a link between concepts from the point of view of a specific domain in order to specify the particular knowledge.

From a knowledge-based systems point of view, an ontology is "a theory (system) of concepts/vocabulary used as building blocks of information processing systems" [Mizoguchi and Ikeda, 1996]. Formal structures for concepts and vocabularies are of interest in assisting humans in organising, sharing and browsing document collections and also in their potential for supporting inference based on knowledge collections [Chandrasekaran et al., 1999].

Current KM encompasses non-explicit knowledge such as unstructured documents and interviews as well as data-oriented information that has been organised in the form of tangible documents, which is prevalent in first-generation KM. To tackle implicit knowledge is to design concepts and their relationship for a specific setting. Therefore ontology can play a key role in KM such as knowledge organisation, knowledge search and retrieval, knowledge presentation, and knowledge acquisition and structuring. That is the reason why ontology has evolved or changed from previous knowledge systems, i.e. database systems, expert systems, or artificial intelligence systems.

Noy and McGuinness [2003] identified five reasons for ontology development:

(1) To share common understanding of the structure of information amongst people or software agents (communication)

(2) To enable reuse of domain knowledge (reusability)

(3) To make domain assumptions explicit (reliability)

(4) To separate domain knowledge from optional knowledge (specification)

(5) To analyse domain knowledge (specification).

Currently, information overload is one of the important issues knowledge management needs to address because people suffer from the difficulty of choosing the right information quickly and easily in conditions of over-abundant information [Heylighen, 2002]. A lot of information is now circulating around the world in the current era of the Internet in which we use web-based systems and documents. Therefore searching for relevant information is a great task for designers and knowledge management systems are needed to tackle the issue. The use of ontologies may be one of the answers to address the issue .

The main purpose of developing an ontology is to communicate between human and machine [Darlington, 2002]. Human language and machine language are different which results in a communication disconnection between human and machine. Therefore, to overcome gaps of information-gathering channels between human and machine, we have to know how knowledge (not information) evolved in a computer. We, also, should find possible ways to communicate meaning, by means of description, between human and machine in order to share knowledge between humans and machines.

The purpose of ontology development is to provide a means of communication between humans and agents (i.e. computer systems). For humans it represents a means of acquiring knowledge more easily and understanding the knowledge more explicitly. On the other hand, in the communication between humans and computers it can be used as an interaction device between their heterogeneities.

There are number of ontology editors (development tools), from conceptual knowledge modelling to specific domain terminological modelling. One study has surveyed 94 ontology editors [Denny, 2002 and 2004]. For this research it was considered necessary to choose an ontology editor that should be: (1) easy to use for people who are not knowledge engineering experts, (2) able to capture knowledge objects from documents, and (3) capable of knowledge analysis and knowledge modelling.

6.3.2 How has ontology been used in engineering design domains?

The affordances of ontology such as extended communication and sharable knowledge have provided an opportunity not only for specialists in computer engineering fields but also those in engineering design fields to use the methodology. From the general

purpose of development of ontology, people in engineering design have focused on their own usages. The followings are examples of such uses:

(1) To obtain interoperability of knowledge used in different programs (e.g. CAD)

(2) To increase communication knowledge between producers and users (e.g. e-commerce, online procurement)

(3) To integrate and manage various types of knowledge in the design process

(4) Knowledge capture and representation of design rationale.

With regard to the first point, in modern engineering design, designers suffer from handling large amounts of information that exist in different formats. This means that interoperability of a concept is needed for sharing the same meaning in different systems. For example, different CAD systems have different formats to represent the same objects. That makes it confusing and time consuming to coordinate information used in different design environments. Semantic conflicts are an important issue in solving the integration problem.

Cross-functional, distributed design teams use CAD and other tools along with available knowledge to develop the physical form, logic, specifications and all other information that defines a product. Additionally, multiple source vendors, sub-contracted manufacturers, distributors, and sales partners also add value to the product by using existing information and generating more knowledge [Dutta and Wolowicz, 2005]. These resources are typically of different types (databases, expert systems, application software, etc.) because they serve the needs of different domains. Thus, an essential feature of product information is well-defined meaning (semantics) in a particular context. Further, growth in the use of the Internet has facilitated communication between the information resources.

The use of ontology in e-commerce has addressed these issues. It has been an early-adopted area of ontology because of the commercial benefit. Ontology provides, for example, interoperable tools for communication of engineering catalogues.

With regard to point (3), there are usually several independent information resources in a design process. In order to integrate systems, ontologies can be used to facilitate representation of different systems [Patil et al., 1992]. Such integration is especially important in the design of product/manufacturing process management systems (e.g. Product Lifecycle Management) in which various stakeholders participate. It is

essential to take into account all kinds of knowledge from various stages of the process in the development of a product. This requires a meaningful formal representation of product data semantics throughout the product's lifecycle.

Finally, fundamental and semantic issues that a designer encounters every day include reasoning on a design, such as why a design was chosen and what are alternatives for the design. This refers to design rationale. Design rationale exists in the heads of human designers. In order to capture design rationale we have to have discourse with a person who has the knowledge. Sometimes that exists in the form of unstructured speech or text, e.g. engineering documents, interviews, conversations, memos, emails or meetings that present designers' rationale in the design processes. Ontologies have been designed to help the reasoning process with identifying and reconstructing the knowledge contents from such unstructured formats.

6.4 The value of developing an ontology on design and error

To examine the value of an ontology is to answer the following questions:

(1) Why will the developed ontology help people?

(2) How will the developed ontology help people?

The first question is related to how to provide people with effective reasoning methods to understand the concept of design-induced error. This is how to overcome a difficulty of a domain analysis of psychological theories on unstructured documents. It needs clear structure and relations of the concepts.

The second question concerns methodologies that extract and show the knowledge. A number of methodologies have been developed to help people to understand knowledge in effective ways. These include visual representation tools (e.g. tree-style hierarchy browser, diagram showing relations graphically), and an annotation (mark-up) system.

The main user of the methodology developed in this research would be a designer. Designers may not have enough knowledge about psychology e.g. human error theories, and the methodology would assist them in taking such theories into account in their work. They have questions on human–system interaction failures but suffer from reasoning about why the operator has done inappropriate things that were not expected

by the designer. These errors could not be predicted, calculated or simulated using general engineering methodologies because they are related to psychological and behavioural phenomena.

It still is a difficult and time consuming task to extract relevant knowledge from accident reports even if designers do have knowledge of psychology. It is also the same for experts, e.g. accident analysts or related researchers. The developed ontology may help them to search for interesting areas of reports faster than before. The ontology therefore should be easy to use, easy to understand, and straightforward to format in terms understandable to, for instance, an engineer

Finally, authorities that produce accident reports may gain a benefit from developing ontologies. There are a number of different formats in accident reports according to which authority produces them. It is difficult and moreover not reasonable to accord such diversity of formats into a fixed formation. That reduces the usability of documents. An ontology is an alternative because it can be developed in a number of styles as required.

Usability is important for accident report providers. If we develop a particular ontology for a certain domain, a researcher has a tool to search accident reports more effectively or easily than before. Ontology does not damage an original description in the document by annotating with a mark-up language. Current data-based analysis systems have to decompose descriptions into data sets resulting in loss of the original description. That makes it difficult for other researchers to try to analyse the material in a different way.

There are many different points of views which analyse a document. An analyst, for instance, wants to know relations between engineering design and accident types. Another analyst needs to analyse physical conditions of operators which lead to errors. Different perspectives can apply to interpret a symptom or relations. Psychologist tries to translate an accident in a manner from engineers. Therefore, it is better to leave an original paper undamaged. However, if the documents remain in unstructured text formats, it is an issue how easily to access documents that they want to find.

The difficulty can be overcome by using annotation methodologies with a mark-up language technique in a current web environment. Ontology plays the role of a template for the application of the annotation.

Therefore, the values to develop ontology in this thesis may be summarised as follows;

(1) To provide a methodology to recognise psychological knowledge

systematically from accident reports in an easily accessible format that can be used in knowledge management systems

(2) To provide multiple view points on an accident

(3) To facilitate knowledge transfer from authorities to ontology browsers in a web site

(4) To help readers to access knowledge effectively by representing related issues in a visual form

(5) To visualise the relationship(s) between design and error

(6) To define terminologies related to design issues with human error,

Chapter 7. Development of an ontology of design-induced error

The previous chapter reviewed the advantage of knowledge sharing and organisation methods in the current knowledge-management system environment. This present chapter concerns the application of the method discussed in the previous chapter to the development of a knowledge-based "*theory based ontology of design-induced error*" which specifies in detail a representation for capturing design issues relating to human error from accident reports.

As has been discussed, there are a number of reasons to develop ontologies in knowledge management systems. In this thesis, the development of the ontology was carried out to provide the designer with an effective methodology to recognise and search for the concept of design-induced error and related design issues from accident reports as well as to gain a better understanding of the concept. This aims translated into the following objectives:

(1) To formalise relations between design of a system and human error in light of the concept of design-induced error by analysing accident reports
(2) To examine the possibility of capturing psychological knowledge from text documents
(3) To demonstrate a knowledge model showing relations between design and error and a process of design-induced error in effective forms (e.g. a visual form).

For this purpose, a "design induced error ontology" has been developed in this research. The ontology includes three parts in order to reveal domain knowledge in these subject areas that could be applied to searching for related issues in the context of accident report documents as a basis for support of the design-induced error reasoning process. These three parts are; the error-inducing design ontology part, the design-induced error theory ontology part and the human- error ontology part.

This ontology development process was conducted by the author and after discussion with supervisors and a knowledge engineering expert at the University of Cambridge.

7.1 Methodologies

For the research, to extract useful knowledge from accident reports for delivering to designers and sharing the knowledge obtained with designers, theoretical and technical methodologies are adopted.

(1) Theoretical methodology

a. Meta-theory of design-induced error (Chapter 4)

b. Knowledge acquisition and modelling process [Milton et al., 1999]

c. Logical ontology development methodology [Noy and McGuinness, 2003]

(2) Technical methodology

a. PC PACK: for generating the ontology, knowledge acquisition, and knowledge representation development [O'Hara et al., 1998; Shadbolt and Milton, 1999]

b. Protégé 2003[18]: for building an open source implementation of the developed ontology [Noy et al., 2000]

PC PACK was chosen for the main technical methodology for this research because it provides tools that are necessary for this research (e.g. a protocol tool for knowledge extraction from documents, diagram and ladder tool for knowledge modelling, and a publishing tool for annotated web pages). This research focused on the knowledge acquisition and knowledge modelling of related concepts rather than taxonomical or ontology languages (e.g. RDF, OWL). PC PACK has been used in many engineering design fields as well as other domains for knowledge construction. According to Denny [2002 and 2004], PC PACK provides easy and useful tools (e.g. by providing highlight pens in a protocol tool) for users (even for non-experts of knowledge engineering) to extract knowledge objects from documents (Table 7.1).

[18] Download from http://protege.stanford.edu/

Tool	Modelling Features/Limitations	Base Language	Web Support & {Use}	Import/ Export Formats	Graph View	Consist-ency Checks	Multi-user Support	Merging	Lexical Support	Inform-ation Extract-ion	Comments
The software tool for editing ontologies	The representational and logical qualities that can be expressed in the built ontology	The native or primary language used to encode the ontology	Support for Web-compliant ontologies (e.g., URIs), and {use of the software over the Web (e.g., browser client)}	Other languages the built ontology can be serialized in	The extent to which the built ontology can be created, debugged, edited and/or compared directly in graphic form	The degree to which the syntactic, referential and/or logical correctness of the ontology can be verified automatically	Features that allow and facilitate concurrent development of the built ontology	Support for easily comparing and merging independent built ontologies	Capabilities for lexical referencing of ontology elements (e.g., synonyms) and processing lexical content (e.g., searching/filtering ontology terms)	Capabilities for ontology-directed capture of target information from content and possibly subsequent elaboration of the ontology	Pertinent information about methodology, availability and support, additional features, etc.
PC Pack 4	Knowledge acquisition and modelling. Multiple inheritance; n-ary relations; rules and methods. User definable templates for modelling formalisms like CommonKADS and Moka.	XML	{HTML output via XSLT}	XML	ER diagrams; class hierarchies; OO views	Only logically consistent models can be created.	Yes	No	No	No	Suite of many integrated KADS inspired tools.
Protégé-2000	Multiple inheritance concept and relation hierarchies (but single class for instance); meta-classes; instances specification support; constraint axioms ala Prolog, F-Logic, OIL and general axiom language (PAL) via plug-ins.	OKBC model	Limited namespaces; {can run as applet; access through servlets}	RDF(S); XML Schema; RDB schema via Data Genie plug-in; (DAML+OIL backend due 4Q'02 from SRI)	Browsing classes & global properties via GraphViz plug-in; nested graph views with editing via Jambalaya plug-in.	Plug-ins for adding & checking constraint axioms: PAL; FaCT.	No, but features under development.	Semi-automated via Anchor-PROMPT.	WordNet plug-in; wildcard string matching (API only).	No	Support for CommonKADS methodology.

Table 7.1 Features of PC Pack and Protégé ontology builders (extracted from Denny, 2004)

PC PACK also supports building of an ontology template for a MOKA[19] [Stokes, 2001] type ontology that is familiar to engineering designers.

PC PACK is an integrated suite of knowledge tools designed to support the acquisition and use of knowledge. It can assist people who want to capture knowledge to produce an intranet site or to develop a knowledge-based system, such as an expert system with the following activities:

• To analyse knowledge from documents

• To structure knowledge using various knowledge models (such as trees, diagrams, grids and hypertext)

• To acquire and validate knowledge from experts

• To publish or implement the captured knowledge

• To re-use knowledge across different subject areas and domains.

There are 10 toolkits in PC PACK as shown in the diagram (Figure 7.1) including the following main tools.

The **Protocol Tool**, which is used to analyse documents

The **Ladder Tool**, which is used to construct hierarchical diagrams (trees/ladders)

The **Diagram Tool**, which is used to construct diagrams

The **Matrix Tool**, which is used to construct matrices

The **Annotation Tool**, which is used to create structured web pages

The **Publisher Tool**, which is used to create websites

The **Diagram Template Tool**, which is used to define diagram formats.

[19] Methodology and tools Oriented to Knowledge-Based Engineering Applications

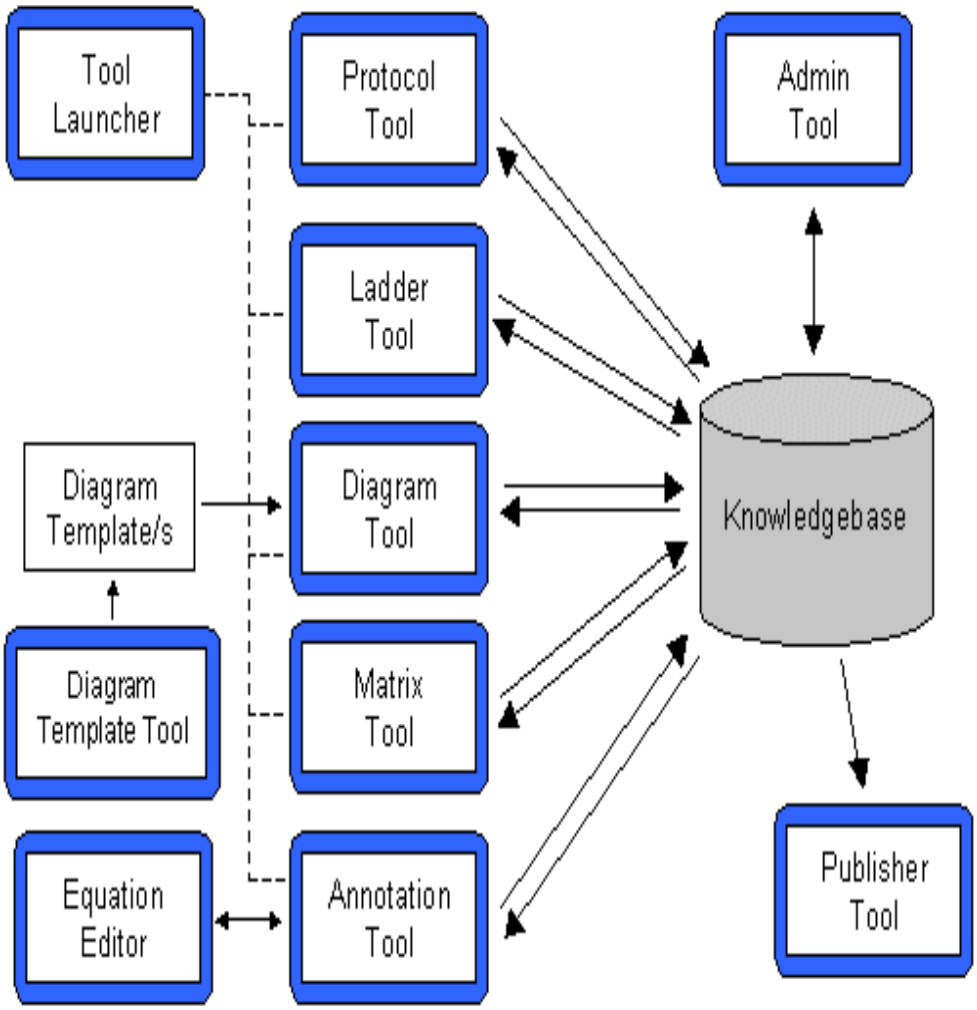


Figure 7.1 A diagram of PC PACK Toolkits (Epistemics[20], 2005)

7.2 Dataset

A collection of accident reports relevant to the concept of design-induced error was essential for the research. There are available sources in websites, mostly government websites (e.g. Air Accidents Investigation Branch, National Transportation Safety Board). When data was gathered it was necessary to consider both the quality and the quantity of the data. For effective research, relevant accident reports that contain the concept of design-induced error need to be gathered because of the need to accumulate the amount of reasonable knowledge relevant to design-induced error.

[20] http://www.pcpack.co.uk/PCPACK5/Help/en/General/pcpackquickguide.htm#usinghelp

ACCIDENT INVESTIGATION BODIES (WEB SITE)	AVAILABLE SOURCES	NUMBER OF INVESTIGATION REPORTS
HSE (Health and Safety Executive, UK; http://www.hse.gov.uk/)	Industrial accident report and reviews	Not available on the web
AAIB (Air Accidents Investigation Branch, UK; http://www.dft.gov.uk/)	Aviation accident reports	37 – full reports
MAIB (Marine Accident Investigation Branch, UK; http://www.dft.gov.uk/)	Marine accident investigation reports 29 (2003), 40 (2002), 41 (2001), 40 (2000), 18 (1999)	168 – full reports, with some short reports
NTSB (National Transportation Safety Board, USA; http://www.ntsb.gov/)	Aviation, railway, highway, marine, pipeline and hazardous materials, accident investigation reports in USA	For Aviation only – Database: 140,000 Full reports: 41 (for 10 years)
ATSB (Australian Transport Safety Bureau, Australia; http://www.atsb.gov.au)	Aviation (678), railway (21) and marine (205) accident investigation reports in Australia	904 – some short reports
TSB (Transportation Safety Board, Canada; http://www.tsb.gc.ca)	Aviation accident reports (476) 5 (2003), 40 (2002), 62 (2001), 66 (2000), 40 (1999), 48 (1998), 46 (1997), 47 (1996), 44 (1995), 66 (1994), 12 (1990-93) Marine accident reports Rail accident reports Pipeline accident reports	Aviation: 476 – full reports with short reports Marine: 255 (1990–2003) – short reports Rail: 88 (1995–2003) Pipeline: 11
OSHA (Occupational Safety & Health Administration, USA; http://www.osha.gov/)	Industrial accident investigation reports in USA	Not available on the web
US Chemical Safety and Hazard Investigation Board (http://www.cbs.gov)	Chemical accident reports in USA	24 (1998–2004) - full reports

Table 7.2. Available sources of accident reports on the web, as at December 2004.

After reviewing several sites (Table 7.2) the Australian aviation accident/incident reports (available at website http://www.atsb.gov.au/) were selected for this research. The reasons for choosing the Australian accident aviation reports for a dataset in this research are that (1) the reports are well formatted in HTML, (2) the descriptions in documents contain more relevant terminologies for searching the concept of design-induced error than other accident reports systems, and (3) they have a larger number of cases than other authorities for developing an ontology in research levels.

7.3 Development of the ontology of design-induced error

Issues addressed in research for the development of any form of a knowledge-based system concern a clear definition of knowledge objects, knowledge elements, and knowledge processes [Hicks et al., 2002]. Epistemics proposes a PCPACK knowledge acquisition process (see Figure 4.1). Noy and McGuinness [2003] suggested the following ontology development steps: (1) determine ontology domain and scope, (2) consider reusing existing ontologies, (3) enumerate important terms in the ontology, (4) define the classes and class hierarchies, (5) define the properties of classes-slots, (6) define the facets of the slots, (7) create instances.

Through discussions with knowledge engineering experts and examination of current methodologies, the following development process was adapted as shown in Figure 7.2. As steps for ontology development, the methodology developed by Noy and McGuinness [2003] was in general adopted here. As a knowledge acquisition and modelling process, the PCPACK process was used. Details of steps of the knowledge acquisition and ontology development process will be addressed in the remaining sections of this chapter.

Initially, the domain and scope of the ontology needed to be determined. Considerations of constraints of the development of the ontology were the main concern in this stage such as: (1) this is a new type of ontology that should provide designers with an insight into knowledge about design issues with human error; (2) the ontology is based on psychological theories; and (3) it is focused on accident reports. From those considerations a conceptual map of the ontology and important terms was drawn.

Secondly, knowledge elicitation followed. Knowledge is difficult to capture as well as to understand. It is necessary to conduct a knowledge elicitation process in order to find: (1) what kinds of knowledge exist in the design-induced error domain, (2) how to and what is the best way to clarify the knowledge, and (2) what are key concepts in the knowledge. There are a number of ways of knowledge elicitation, e.g. interview, survey, brainstorming and so on. This research adopted a description analysis of accident documents as a knowledge elicitation process because the main purpose of this research is how to capture relevant knowledge from accident reports. This analysis examined the contents of accident reports in order to identify accident reports that contain design-induced error.

The characteristic words or phrases that present design-induced error were determined

and then extracted from the accident reports for categorising an ontology of design-induced error. With this process of testing, documents (domain documents) that might be considered to contain the concept of design-induced error were selected for the next steps.

Thirdly, concepts and relations were generated with the PC Pack ladder toolkit [Milton et al., 1999] based on the results produced in previous steps. A knowledge acquisition and modelling process was followed. These tasks adopted knowledge representation methodology with PC Pack protocol, diagram, and annotation toolkits.

Finally, by conducting a verification and validation of the developed annotation and web browser, and by refining the concepts and relations several times, an ontology of design-induced error was formulated. This process led to the publication[21] of web browseable design-induced error ontology.

This study used a web-based ontology methodology (i.e. PC Pack) because of considerations of usability of the ontology.

[21] The web browseable ontology is not yet published externally but available in an internal system only.

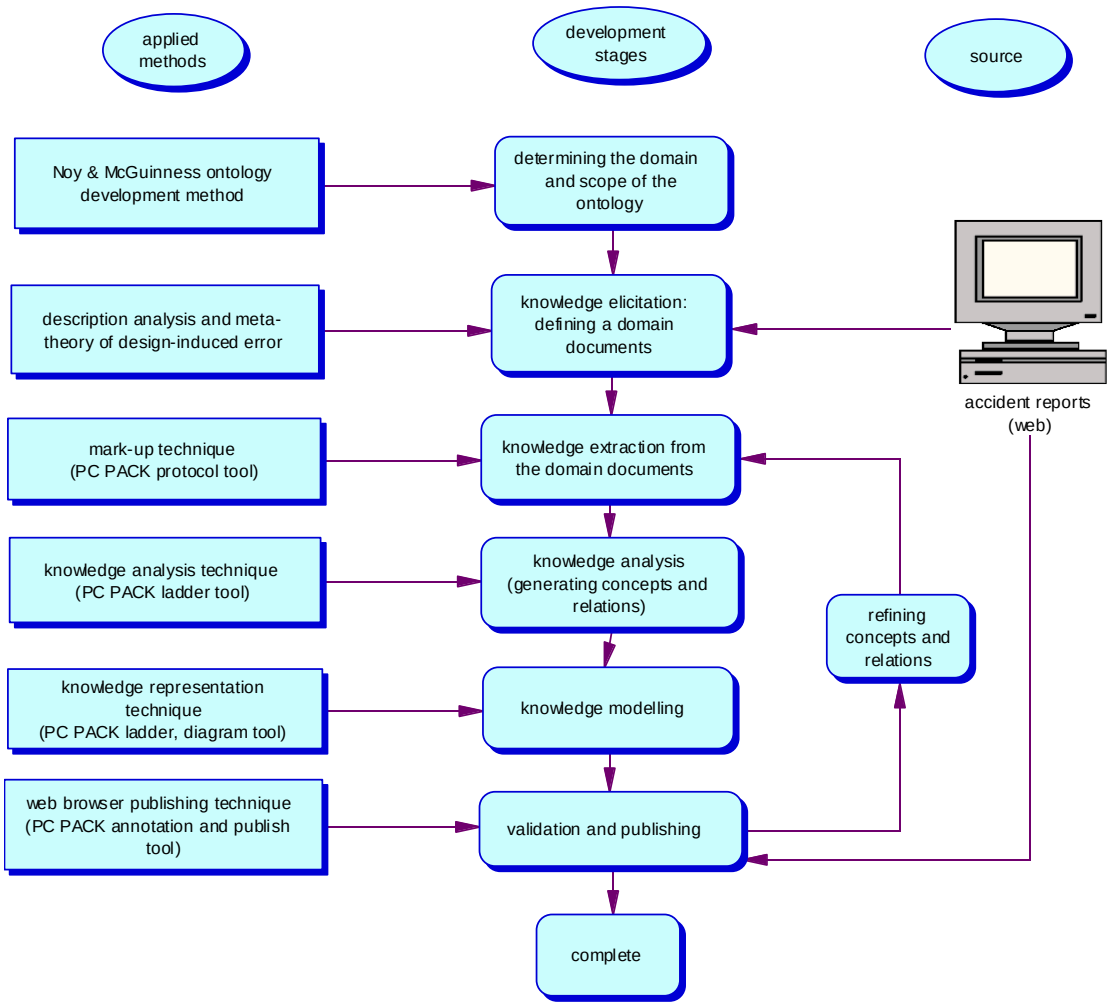


Figure 7.2. Process of ontology development and applied methods

7.3.1 Stage 1: Determining the domain and scope of the ontology

A first step to develop an ontology is to determine the domain and scope of the ontology [Noy and McGuinness, 2003]. The domain of the ontology is determined by identifying the purpose of the ontology. This research concerned how to provide an effective tool for reasoning on human–system interaction failures by developing relevant knowledge extraction and representation methodology to find design issues related to human error from accident reports.

In order to determine the scope of the ontology of design-induced error, a list of questions that a knowledge base based on the ontology should be able to answer was sketched as competency questions **[**Gruninger and Fox, 1994]. In the design and human

error domain, The followings were created as possible competency questions: (For designers, researchers, and authorities producing accident report systems)

(1) Which terms can we find in accident reports that represent the concept of design-induced error?

(2) Which design-induced error characteristics should I consider when designing a system?

(3) How do operators think about a system when I design the system in order to prevent accident and increase safety?

(4) How does design lead operators to make an error? Which design concept can make operators fall easily into design-induced error phenomena (e.g. gulf of evaluation)?

(5) Is there any case that shows trust in automation phenomena? For example, does trust in automation occur in GPS systems?

(6) What kinds of design-induced error are related to a particular design e.g. the Flight Management System?

(7) What kinds of design factors related to automatic systems contributed to operators' inability to solve a problem?

(8) What are the different perspectives between designer and operator in human–system interaction failures?

These questions will serve as the litmus test during development: Does the ontology contain enough information to answer these types of questions? Do the answers require a particular level of detail or representation of a particular area? Thus we can conclude as follows:

- **The domain covered by this ontology**: Accident reports, especially Australian aviation accident and incident reports (see Table 7.2).

- **The purpose of the developed ontology**: To assist in searching for and identification of relevant design issues in human error (human–system interaction failures) cases in accident reports.

Reuse of existing ontologies was considered but unfortunately a relevant reusable ontology was not found. The ontology had to be developed from scratch. However, it

is necessary to mention that this process is important in development of ontology. There are a number of ontology libraries (e.g. the Ontolingua[22] or DAML libraries[23]) from which people can import relevant existing ontologies for their own ontology development.

7.3.2 Stage 2: Knowledge elicitation: Defining testing documents

Although the domain and scope of ontology was determined, there was no clue as to how to construct the ontology of design-induced error to be identified. In order to tackle the problem, it is necessary to elicit relevant knowledge concepts from existing domain knowledge or experts. It is said that the knowledge elicitation process has an important advantage in order to develop an ontology [Gruber, 1993]. This process helps to identify the domain of knowledge that people want to capture and organise.

There are a number of knowledge elicitation methodologies, e.g. an interview with domain experts, a brainstorming with experts, or collecting documents that contain domain knowledge [Liou, 1990; Milton et al., 1999]. The research adopted a manual description analysis of accident reports as a knowledge elicitation methodology because a knowledge source in this research is accident reports. This process was conducted by the author and by discussion between the author and experts in design and human error at the Innovative Manufacturing Research Centre (IMRC) at the University of Bath. The process examined and analysed accident reports in terms of the concept of design-induced error in order to identify relevant knowledge structures for constructing the ontology by the following process (Figure 7.3).

(1) Screening for documents that contain "*human–system interaction failure*" by picking up cases that were caused by "operator error".

(2) Analysing the screened cases in terms of design-induced error by applying theories identified in Chapter 4.

(3) Clustering necessary concepts (e.g. error-inducing design, human error) for the

[22] http://www.ksl.stanford.edu/software/ontolingua/

[23] http://www.daml.org/ontologies/

ontology development.

(4) Enumerating important terms (or phrases) by categorising terminology (keywords) that appear frequently or are used to express a concept.

(5) Classifying documents according to evidence.

(6) Selecting domain documents (testing documents) that will be used for the knowledge acquisition and representation process.

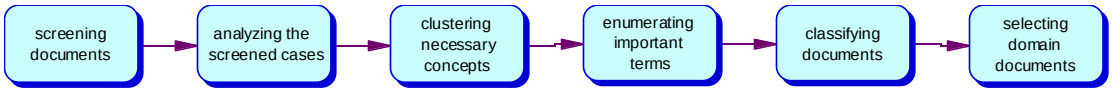


Figure 7.3 Knowledge elicitation process

For the 1st and 2nd step, the author analysed 562 Australian aviation accident reports (Figure 7.5) in the ATSB website (Figure 7.4). The reviewed data set of accidents (from 1995 to February 2005) were entered into the Microsoft Excel spread sheet with 88 column (10 categories, see Appendix A) for the data sheet. Figure 7.6 show part of analysis results; accident types and phenomena.

During description analysis the 3rd step clustering categories of keywords or phases were developed such as defective cognition, performance problem, knowledge problem, distracted cognition, and reliance on systems (see **Table 8.3**). For the 4th step terms and phrases related to theories selected from the accident reports were input to the Microsoft Excel data sheet. These process will be discussed in Section 8.2.

Documents then were classified in the 5th step according to the evidence of design-induced error based on Table 8.1 discussed in Section 8.1. The results of classification of accident cases according to evidence levels shown in Table 8.2. The human error data set then were input to the Microsoft Access database (Figure 7.7).

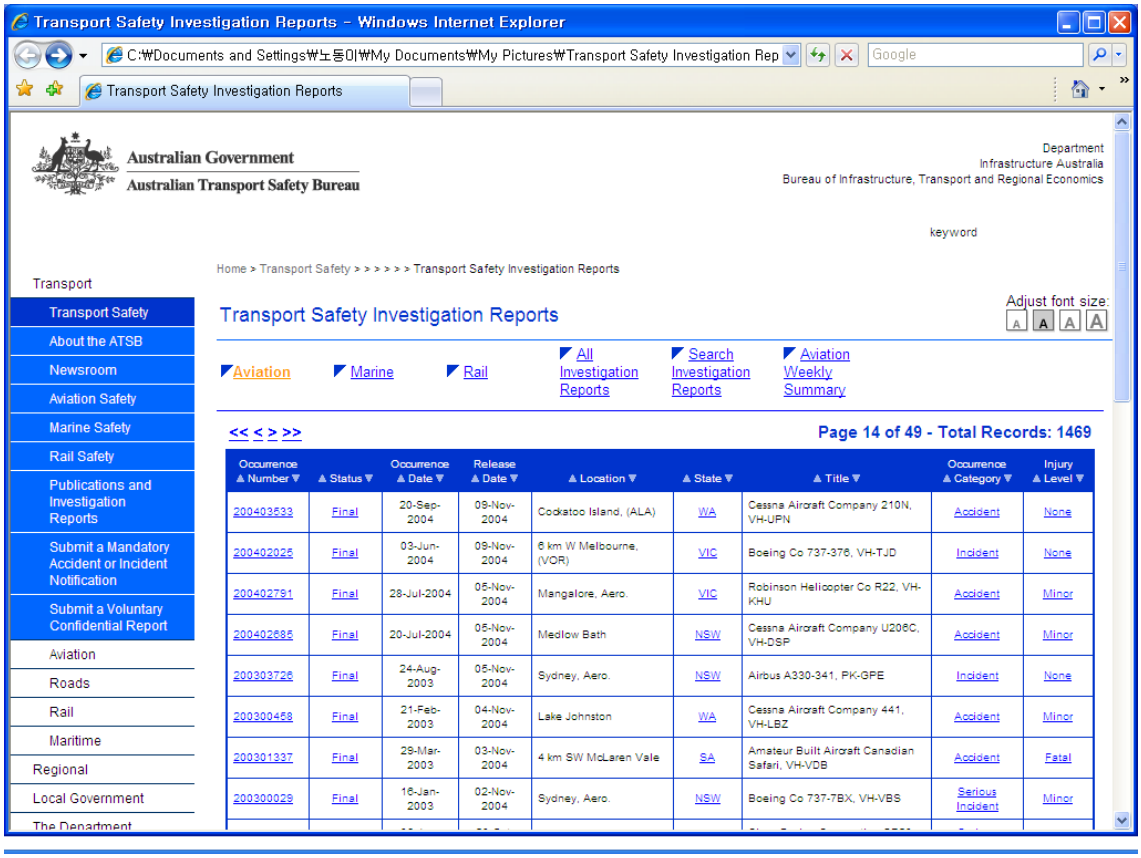
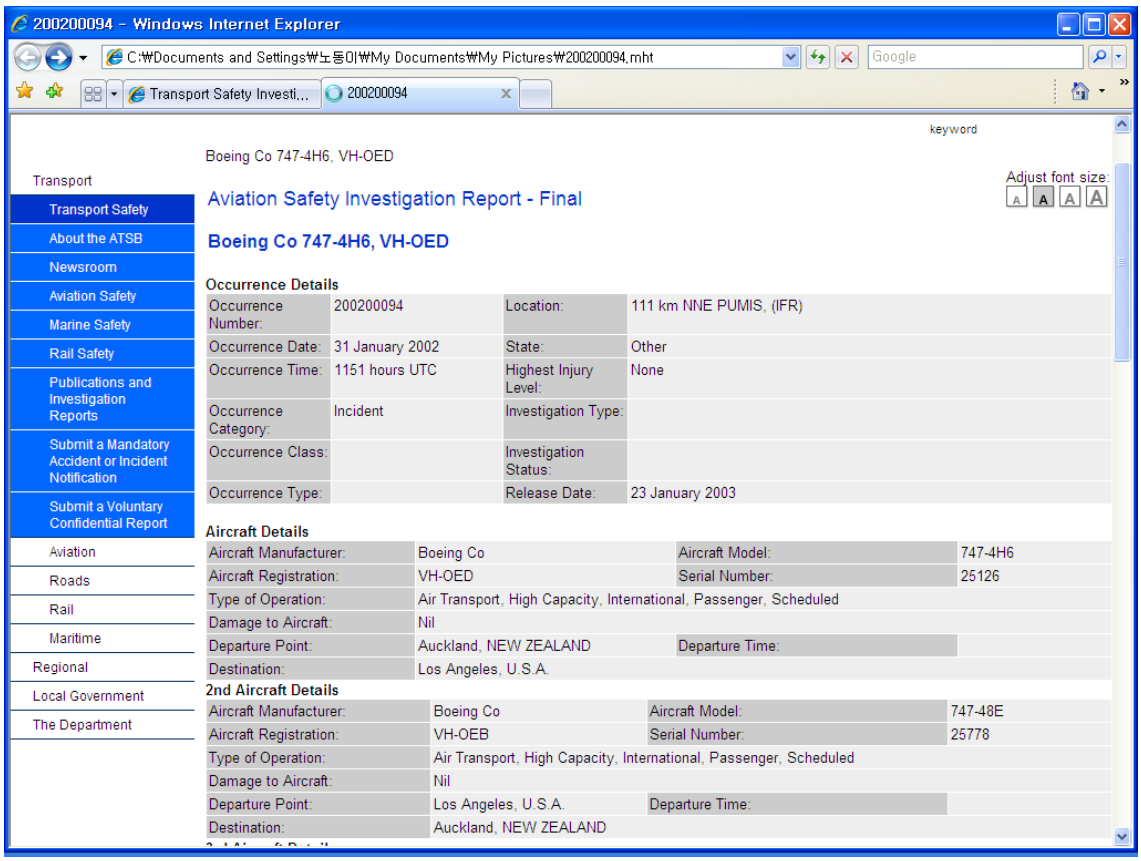


Figure 7.4 A screen shot of the aviation accident report database in ATSB website (list)



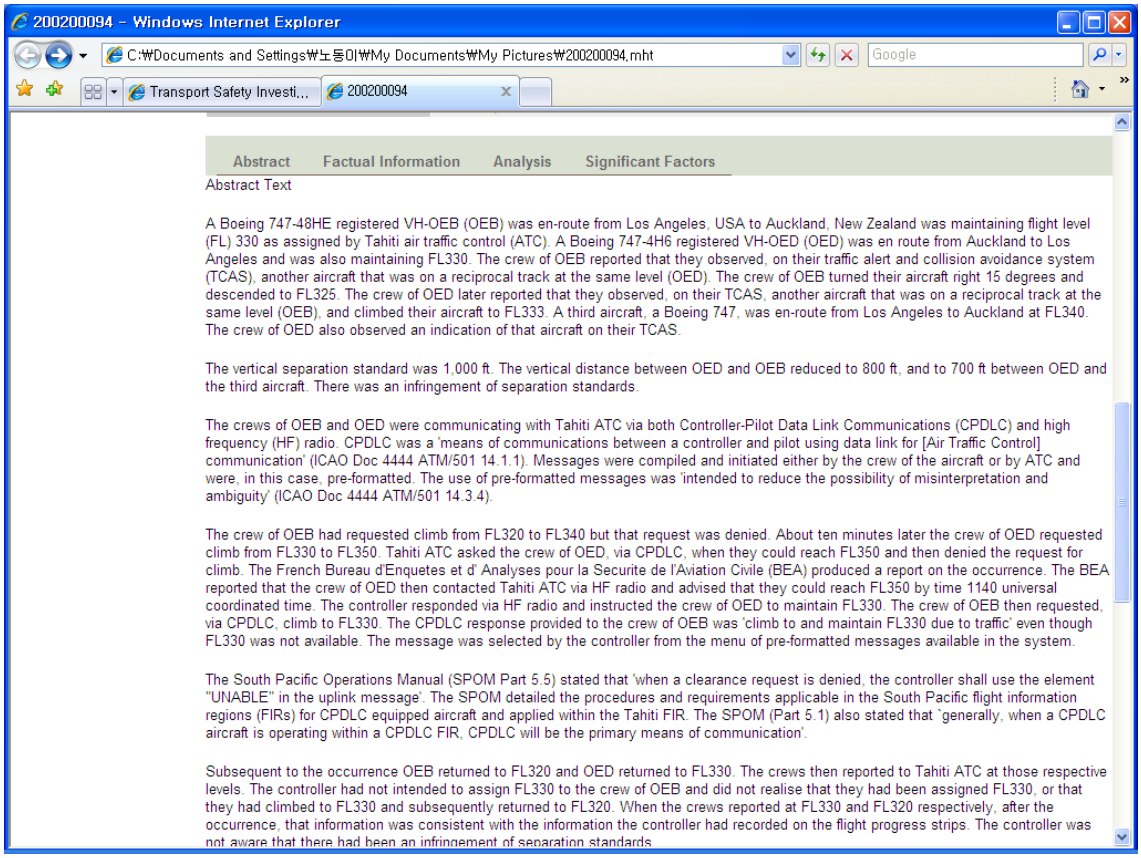


Figure 7.5 A screen shot of an aviation accident report in ATSB website (a case)

name of accident	gulf of execution	gulf of evaluation	plan delegation	design affordance	irony of automation (in	irony of automation (m	trust in automation	automation surprise	risk homeostasis	mechanical failure	operator failure	external factor	unknown
200302847					1						1	1	1
200304091													1
200403720	1								1		1		
200403210		1	1								1		
200403210	1			1							1		
200402749										1			
200305496													1
200404700		1	1								1		
200402049	1		1								1		
200404286		1		1							1		
200402714		1		1							1		
200404460	1			1							1		
200401411		1	1							1	1		
200304918										1			
200302433	1						1				1		

Figure 7.6 A snapshot of part of the Ms Excel spread sheet

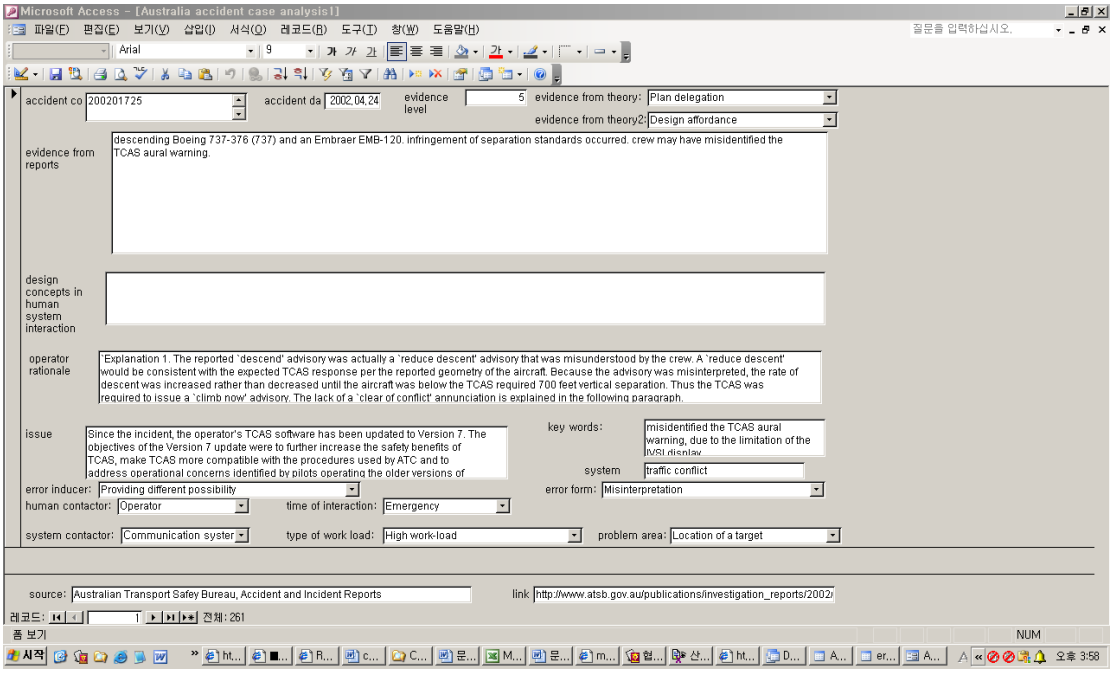


Figure 7.7 A snapshot of the Ms Access database

Result: 562 cases were taken from the Australian aviation accident report web site for analysis and were examined. After conducting the manual description analysis by partly applying a text-mining methodology, 52 cases were then selected as domain documents (i.e. testing documents) for an ontology construction process because these reports were considered as containing descriptions relevant to the concept of design-induced error. The data was marked and saved in a database system (Microsoft Access) for further use and analysis.

7.3.3 Stage 3: Knowledge extraction

A knowledge extraction process was applied to the defined domain documents. The Protocol Tool of PC PACK was used to analyse transcripts of accident reports chosen in the previous stage. The tool provides the means to identify the important knowledge, for example, the concepts, attributes, and relationships as well as instances. The tool simulates the way someone would mark-up a page of text using highlighter pens. Each type of knowledge is associated with a different colour, for example, blue for "design" concept, red for "human error". This process was conducted simultaneously with a knowledge analysis (described in the next stage). Basic concepts, attributes, and relationships were predefined by the knowledge analysis. Terms and phrases in the domain document were extracted as instances of concepts.

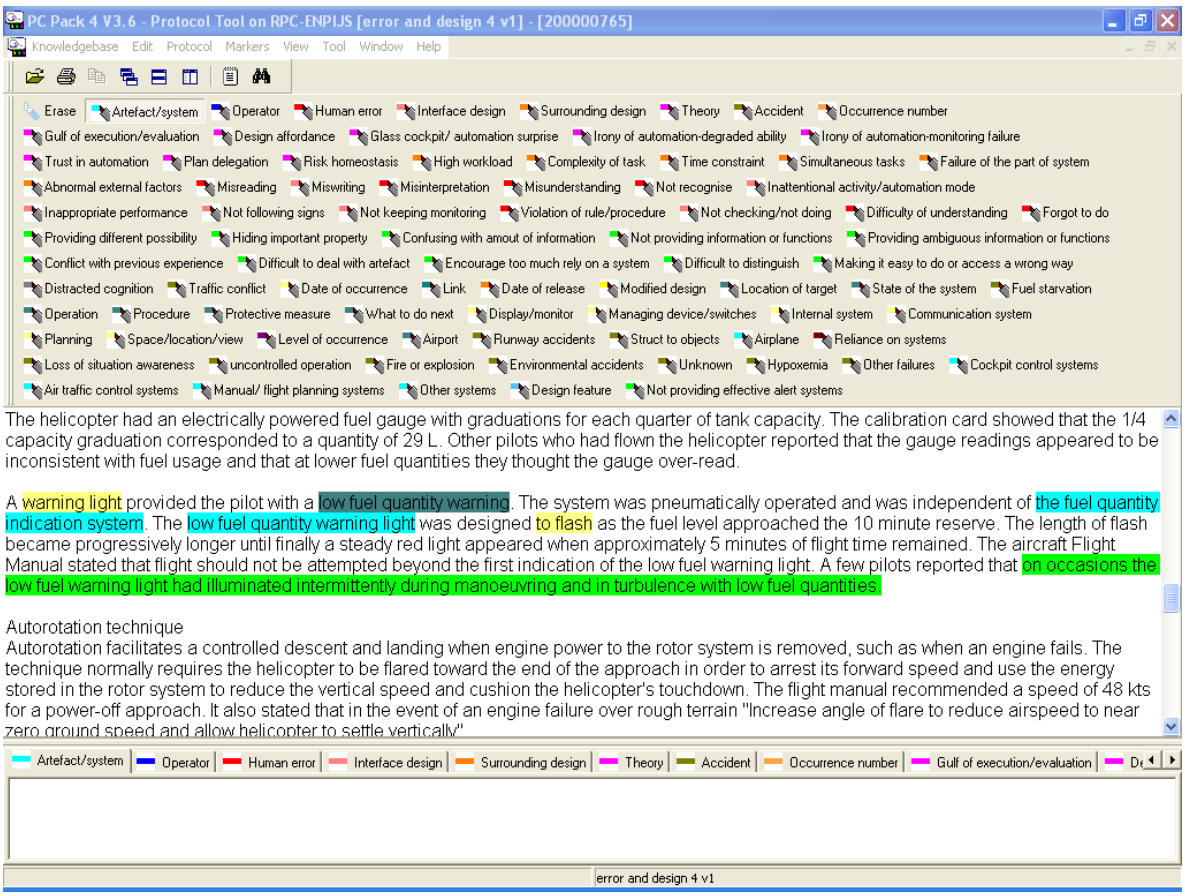


Figure 7.8 A screen shot of the PC PACK protocol tool for knowledge acquisition (mark-up)

7.3.4 Stage 4: Knowledge Analysis: Generating concepts and relations

As discussed in the previous chapter, knowledge analysis is a task to define knowledge objects (concepts, attributes, and relationships). Knowledge analysis and the knowledge extraction process are intertwined with each other.

With the knowledge elicited in the previous stage from the categorisation and decomposition of accident reports, the next stage generated concepts and relations that make an ontology model of design-induced error. This process was to answer questions such as: What are the related concepts located in this process? How many of them can we capture in order to formalise them?

(1) Defining the classes (concepts) and class hierarchy

When we think about a process of human error, the theories related to design-induced error tell us that there are different processes operating – one is from the designer's perspective and the other is from the operator's. Enumerating the classes (i.e. concepts) of the design-induced error ontology starts by considering these processes.

This ontology is based on the meta-theory and on accident reports. The classification of concepts and the class hierarchy are therefore categorised and defined according to how the classification and terminology effectively capture the concepts.

The purpose of this research is to provide people with a methodology of searching for psychological phenomena from accident reports (chapter 1). Since the ontology will be used for extracting knowledge from accident reports it is necessary to adopt as effective a way as possible in order for it to be: (1) familiar to people, and (2) easy to understand and recognise related terms in the accident reports in order to assist searching for the design issues with human error. From this viewpoint the classification pursued for the research needs to accord with both engineering and psychological classification. The terminology and classification adopted in this ontology is not defined correctly according to engineering or psychological terms.

According to the meta-theory of design-induced error (chapter 3) the following assumptions are inducted:

Assumption 1: Design-induced errors are induced by design (design, human error)

Assumption 2: Human error arises from human–system interaction failures (problem area, system)

Assumption 3: Theory can explain such failures (theory, human error)

Assumption 4: There are different perspectives between designers and operators (designer, operator)

From assumptions 1, the concepts of "design", "human error", from assumptions 2 concepts of "problem area", "human–system interaction method", "system", from assumptions 3 concept of "theory", from assumptions 4 concept of "designer", "operator" are introduced.

In addition, from accident report, concepts of "accident report", "airplane", "aeroplane",

"airport", "airfield", "aerodrome", "accident" are added.

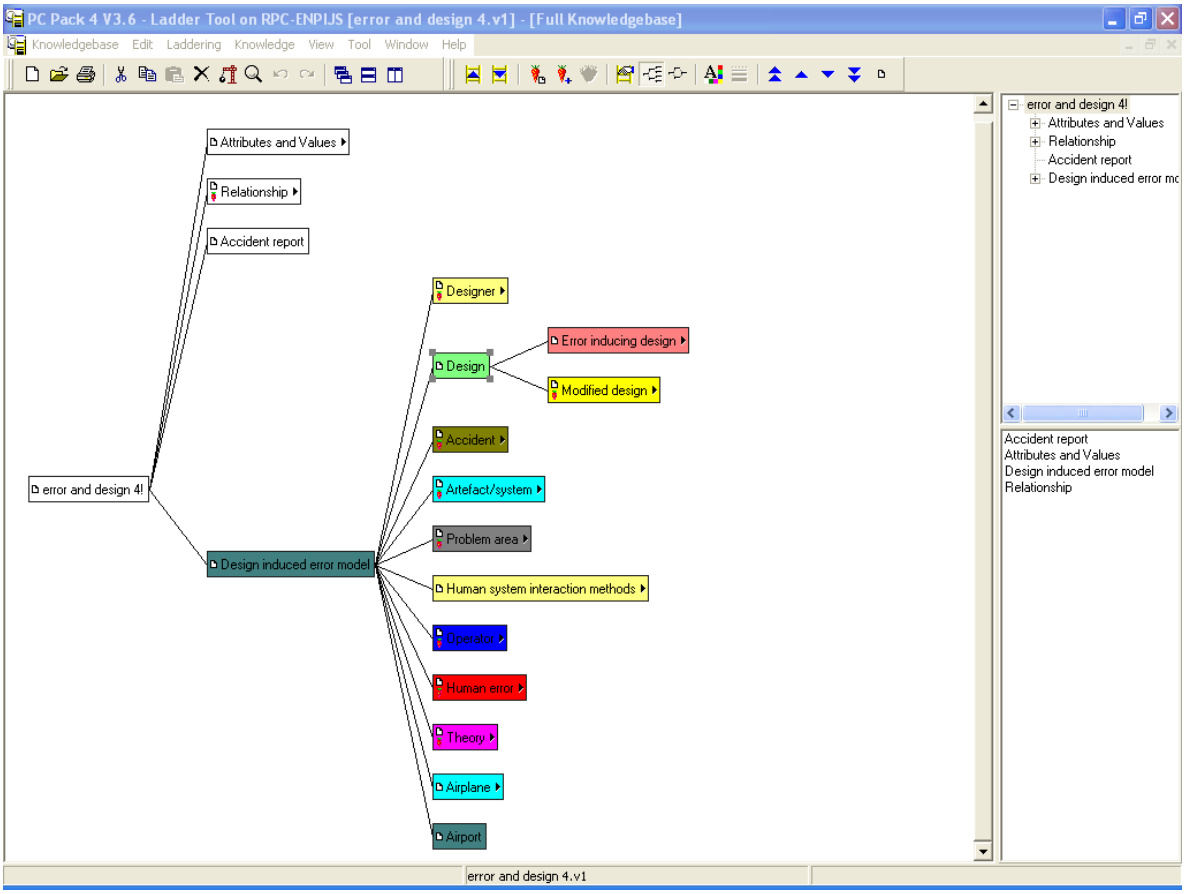


Figure 7.9 A screen shot of the PC PACK ladder tool for constructing an ontology template

With these preliminary defined concept categories, the classes and the class hierarchy were constructed using the PC PACK ladder tool (Figure 7.9). Knowledge captured in the previous step, a knowledge extraction step, can be automatically put into the related concepts.

(2) Defining the relationships between classes

In order to define the relationship between classes an ER (Entity and Relation) diagram was first drawn with concepts (Figure 7.10). This conceptual ER diagram shows how the concepts are relating to each other.

A conceptual ER diagram to express design-induced error could be three parts of entities: designer, operator, and design-induced error theory. From the design part "designer" has perspective "intention" and has "design" " in order to achieve goals.

Designers' ideas are embedded in a "design" that produces a "product" called an "artefact" or "system". The artefact or system provide "human-system interaction method". On the other hand "operator" has perspective of "expectation" on the design for operating the artefact or systems. The operator interacts with "human-system interaction method" in order to reason about "issue". If the issue could not be solved by the operator, it is called "human error" that result in "accident".

Finally, the "design-induced error theory " explains that the relation between design and human error with the different perspectives of designers and operators, and then the intention of designers can be frustrated by a different expectation of operators.

From this conceptual ER diagram, 16 relations were defined (Figure 7.11).

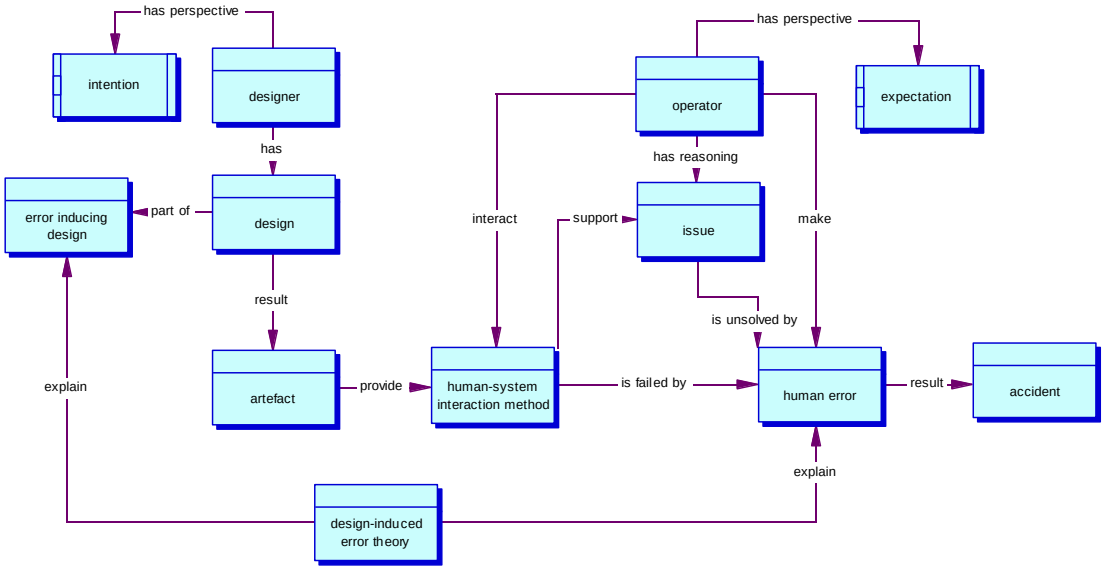


Figure 7.10 The ER diagram of design-induced error process

The PC PACK Ladder Tool and Diagram Template Editor were used to build concept and relation hierarchies (Figure 7.11). The ladder tool provides for construction of a tree-like hierarchical diagram by putting entities into ladders. There are a concept ladder, a relation ladder, and an attribute ladder in the tool.

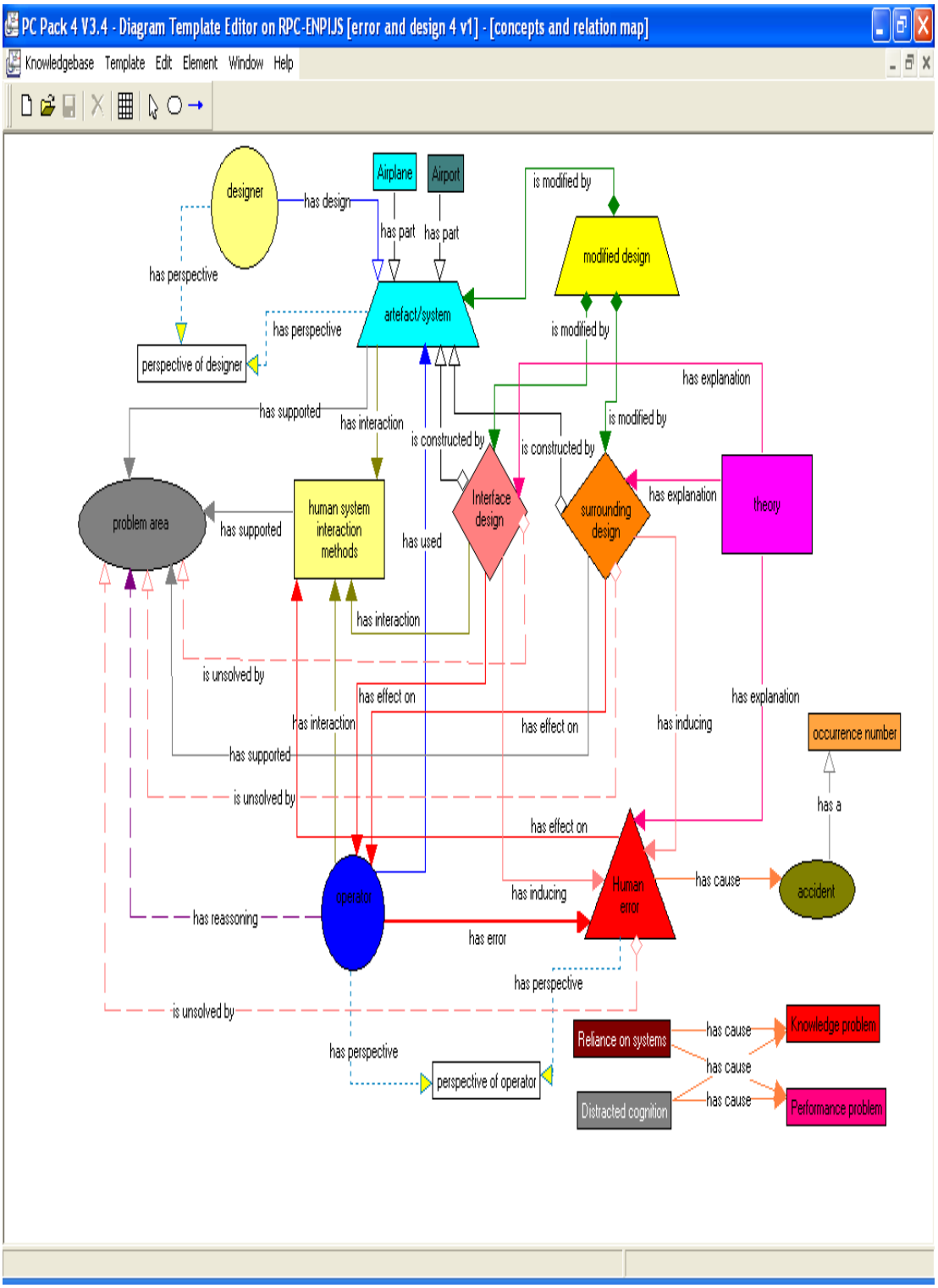


Figure 7.11 A diagram template of relationship between concepts (PC PACK diagram template tool)

7.3.5 Stage 5: Knowledge modelling

The Diagram Tool is used to create and edit diagrams. Concepts and relationships can be represented in the diagrams in the form of nodes and links. Nodes in a diagram represent knowledge objects in the knowledge base, and links represent relationships between the knowledge objects. A diagram template determines the types of nodes and links used in a diagram. Forty accident report documents cases were reconstructed with the tool (Figure 7.12).

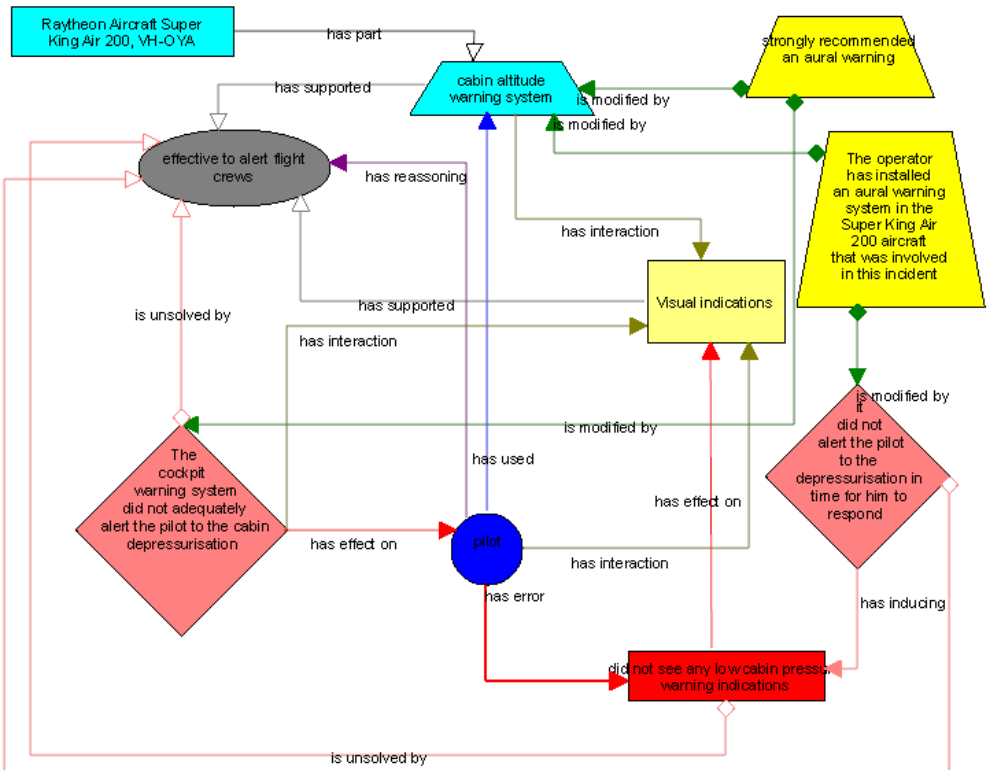


Figure 7.12 A diagram of an accident case (example) constructed by the PC PACK diagram tool

The Annotation Tool allows a page of information to be created and edited for each knowledge object (e.g. concept, attribute, task). The user can enter text or pictures to annotate what is known about that particular knowledge object. The tool uses a hypertext (html) format, hence words can be highlighted and linked to other pages. This allows Worldwide Web-like knowledge-structures to be constructed that can be based on the hierarchies produced in the Ladder Tool (if desired). Templates are used to define the structure, style and contents of annotation pages. These can include special commands to insert information automatically from the knowledge base into the

annotation page.

7.3.6 Stage 6: Validation and publishing of the developed knowledge

This step helped the researcher by allowing previous steps to be look back on to check missed or wrong concepts or relations and then to revisit previous steps in order to modify inappropriate results. Annotated documents were internally published in the form of a website and then the concepts and relations were checked several times. This process should continue for further examples and It is expected that the ontology will be continually refined because the ontology development is not exhausted. Experts in human error and users (e.g. designers) can participate in a further validation process.

The PCPACK Publisher Tool was used to publish the knowledge base of design-induced error on a website (e.g. Figure 7.13). As it was published in this way, PCPACK is no longer required to access the knowledge base. Therefore, it is possible for the knowledge base contents developed to be sent to other people and viewed by them without the need for PCPACK. This research provides 40 cases as instances of the ontology in the knowledge base.

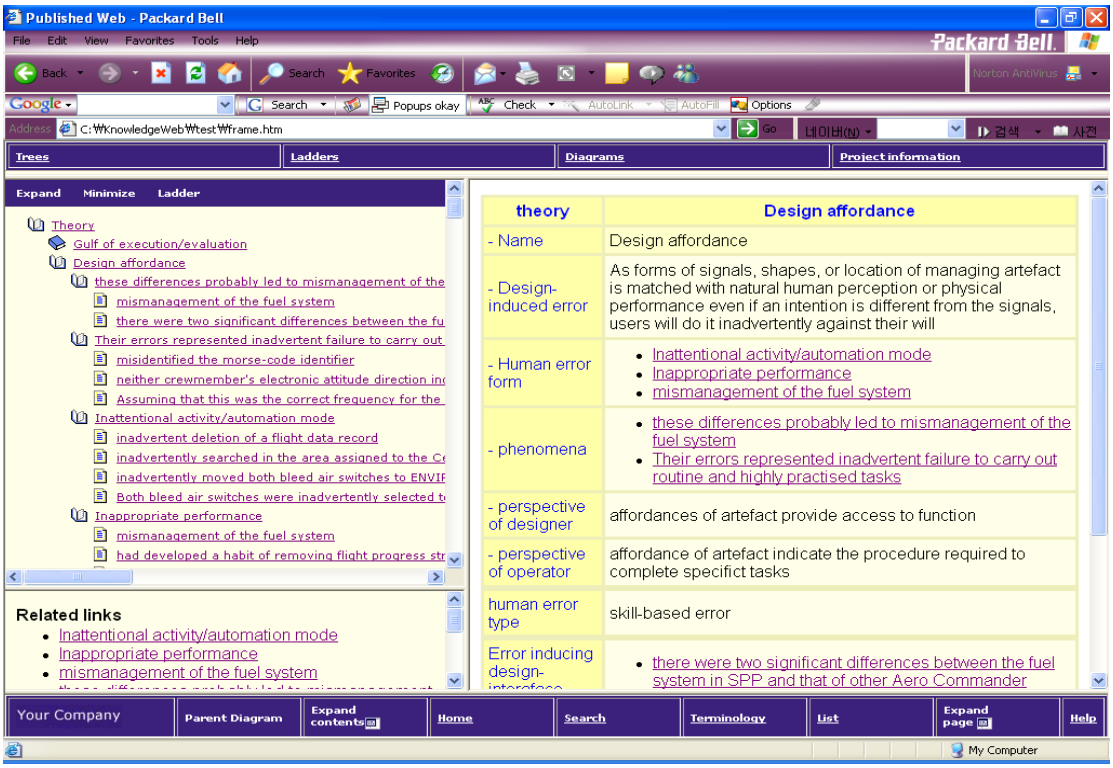


Figure 7.13 The published ontology browser by the PC PACK publisher tool

7.4 The theory-based ontology of design-induced error

With the development steps as described in the previous section, "a theory-based ontology of design induced error" was formulated. This ontology model is proposed to capture design issues relating to the concept of design-induced error in accident reports. It attempts to identify the relationships amongst objects that exist in the domain of the design-induced error. The ontology is intended to represent related concepts of design-induced error and their relations. In the course of the investigation into the use of ontology for capturing the concept of design-induced error, three main parts of the ontology – "error-inducing design part', "human error part", and "design-induced error theory part" – were constructed as the discourse of domain knowledge of design-induced error. This section describes the main concepts and relations in the ontology developed with the three important parts of the ontology;

The error-inducing design ontology part: This part is for identifying design concepts that induce human error.

The human-error ontology part: This part is for what kinds of errors human operators make in human–system interaction failures.

The design-induced error theory ontology part: Each one of these sub-classes contains one of the design-induced error theories with a different viewpoint between designers and operators.

7.4.1 The design-induced error model ontology

This model (Figure 7.14) consists of ten main concepts that appear in the process of design-induced error. The design-induced error process begins from "designers". Designers' ideas are embedded in a "design" that produces a "product" called an "artefact" or "system". The artefact or system performs "operations" in order to achieve goals. In order to operate the artefact or systems, human operators are needed. Their activities are designed to help the artefact/system achieved the goals. However, the "theory of design-induced error" explains that there are different perspectives between designers and operators, and then the intention of designers can be frustrated by a

different expectation of operators. Unintended design outcomes called "error-inducing design" lead human operators to make "human errors" resulting in an "accident" in a real context. There is a "problem area" that human operators encounter when they interact with a system. Figure 7.15 presents main hierarch of concepts.

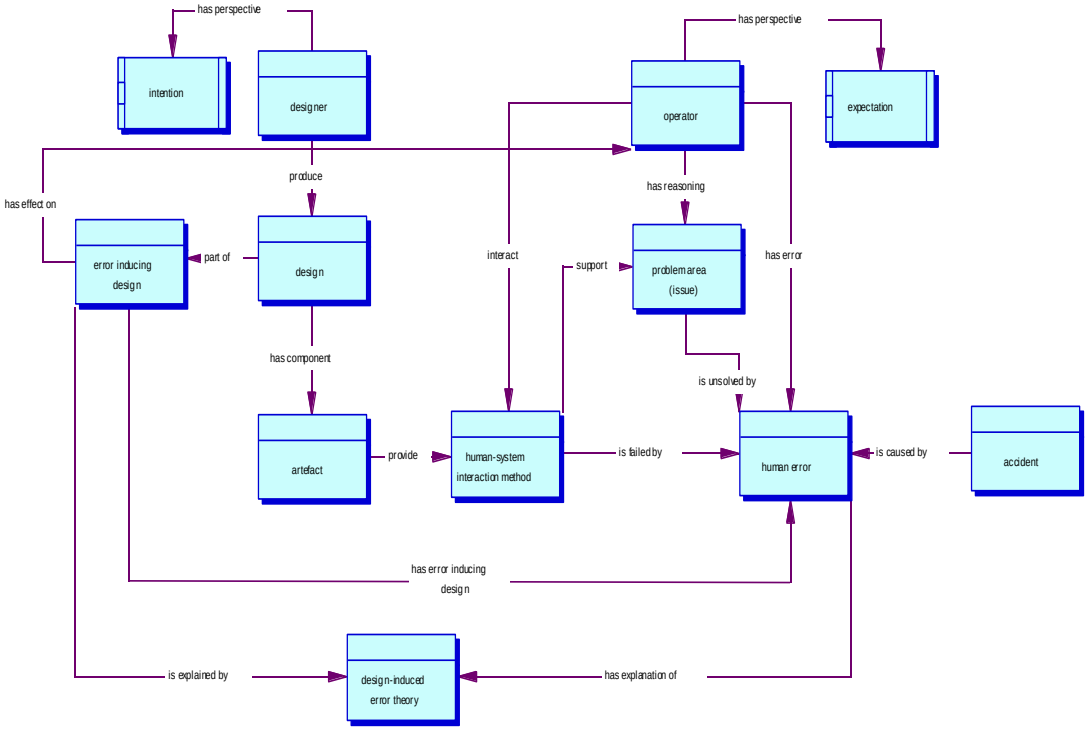


Figure 7.14 An ontology model of design-induced error

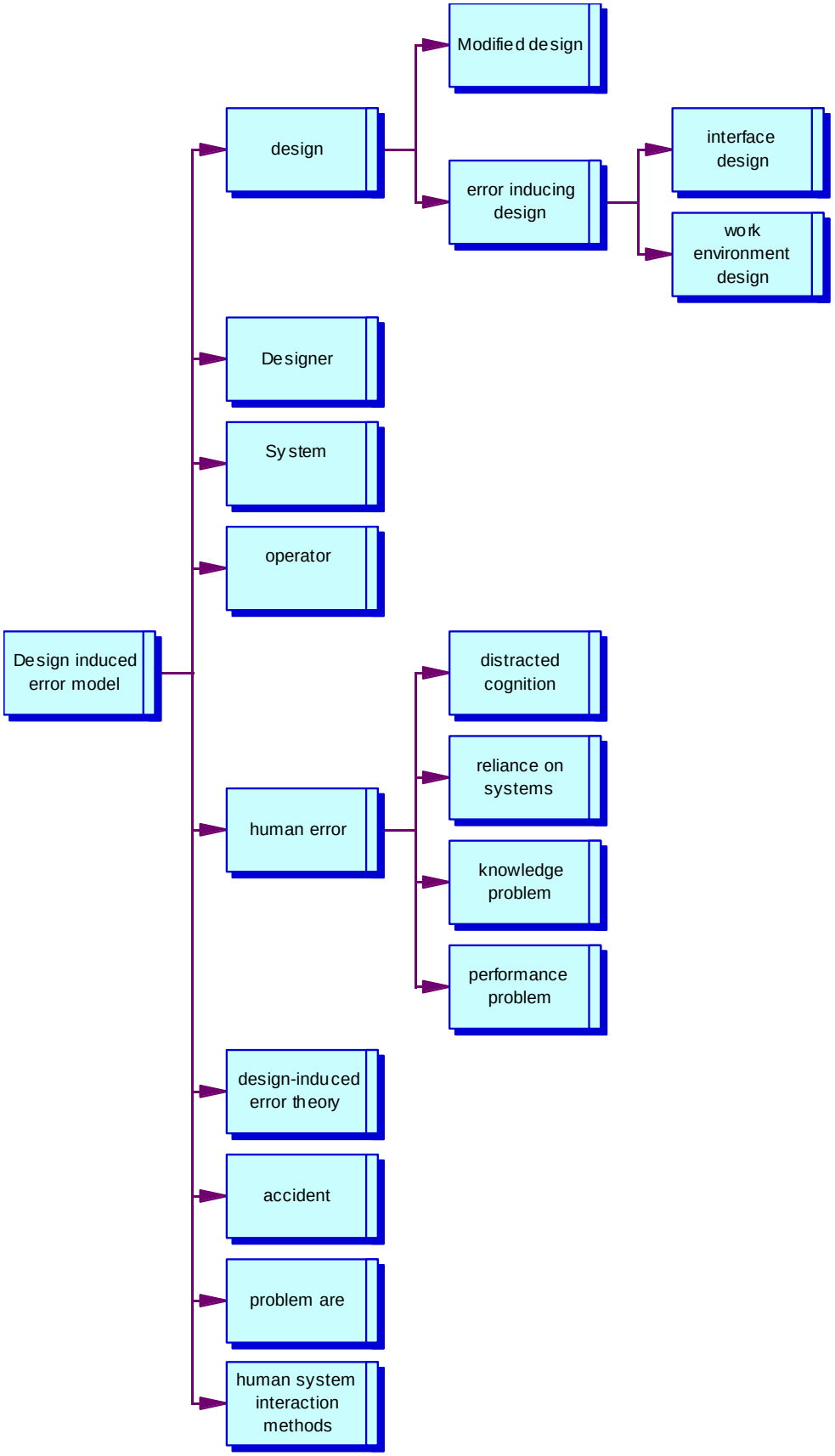


Figure 7.15 The main concept tree of design-induced error

Concepts (classes):

Error-inducing model is the main concept that consists of concepts such as *Accident, Aeroplane, Airport, Date, Design, Designer, Human error, Operator, Problem area, Product, Theory*.

Design concept has *Error-inducing Design* and *Modified design.*

Error-inducing design *has a sub-class of Interface design and Work environment design.*

Interface design concept expresses failed design in direct interaction between human operators and artefact, in which Conflict with previous experience, *Confusing with amount of information, Difficult to distinguish, Difficulty of dealing with artefact, Hiding important property, Increasing dependency on automation, Making it easy to do it the wrong way, Not providing information or functions, Providing ambiguous information or functions, Not providing effective alert functions, and Providing different possibility.*

Work environment design concept expresses failed design that exists in the surroundings of operators and does not need to be directly connected to the error but affects cognition and performance of the operator while conducting a task. *Creating complexity of tasks, Creating simultaneous tasks, Creating time constraint, Creating high workload, Abnormal external factors, and Failure of the other parts of system are sub-classes of work environment design.*

Modified design concept expresses a modification or change of design that was recommended by the investigator or conducted by an operator who is responsible for the system.

Human error concept has four parts*; Distracted cognition, Reliance on system, Knowledge problem, Performance problem.*

Knowledge problem concept has sub-classes of *Misreading, Misinterpretation, misunderstanding, Not recognising, Difficulty of understanding, Forgot to do, Violation of rule or procedure.*

Performance problem concept has sub-classes of *Inattentional activity, Inappropriate performance, Not following signs, Not checking or doing, Miswriting, Not keeping monitoring.*

Problem area concept expressed *Location of target, Operation, Procedure, State of the system, What to do next, and Protective measure.*

Product concept has *sub-classes of Cockpit control system, Traffic control system, Other system.*

Theory concept consist of the theories of*; Gulf of execution or evaluation, Irony of automation (degraded ability), Irony of automation (monitoring failure), Trust in automation, Design affordance, Automation surprise (Glass cockpit problem), Plan delegation,* and *Risk homeostasis*.

These concepts have relations each other. Ten relations are defined in order to express the relevant knowledge of a concept of design-induced error. For example, the concept of error-inducing design has a "has_effect_on" relation with the concept of operators. The concept of human error has a "has_error_inducing_design" relation with the concept of error-inducing design. In Table 7.3 relations between concepts are presented.

Figure 7.16 shows a diagram of concepts and relations in design-induced error ontology. Concept trees are illustrated in Figure 7.17

Table 7.3 concepts and relations

NO	CONCEPT 1	CONCEPT 2	RELATION
1	Operator	Expectation	Has_perspective
2	Operator	Problem area	Has_reasoning
3	Operator	Human-system interaction method	Interact
4	Operator	Human error	Has_error
5	Designer	Intention	Has_perspective
6	Designer	Design	Produce
7	Design	Error inducing design	Part_of
8	Design	Artefact	Has_component
9	Artefact	Human-system interaction method	Provide
10	Human-system interaction method	Human error	Is_failed_by
11	Human-system interaction method	Problem area	Support
12	Problem area	Human error	Is_unsolved_by
13	Human error	Design-induced error theory	Has_explanation_of
14	Error inducing design	Human error	Has_error_inducing_design
15	Error inducing design	Design-induced error theory	Is_explained_by
16	Error inducing design	Operator	Has_effect_on
17	Accident	Human error	Is_caused_by

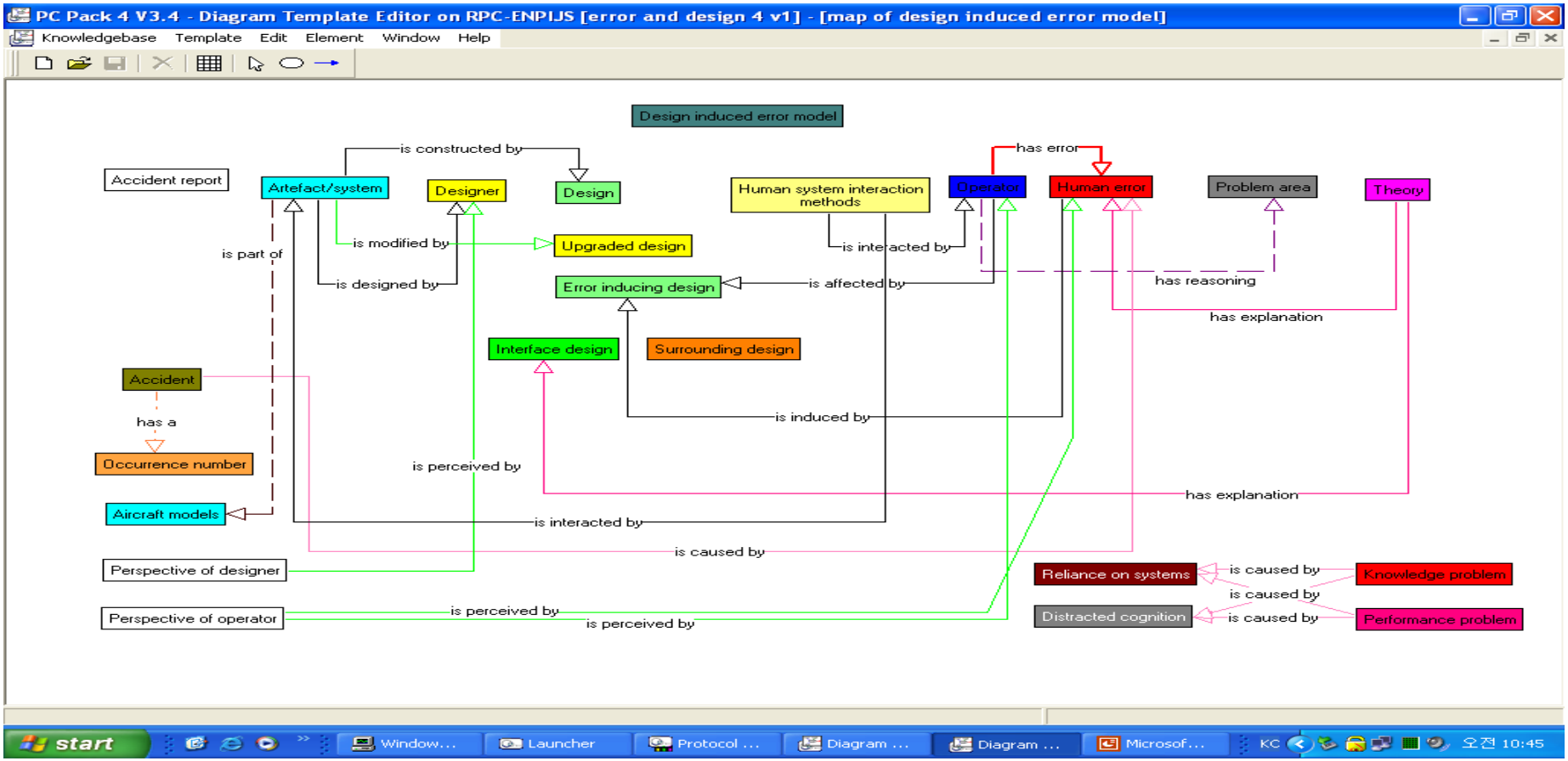


Figure 7.16 A diagram of concepts and relations of design-induced error ontology

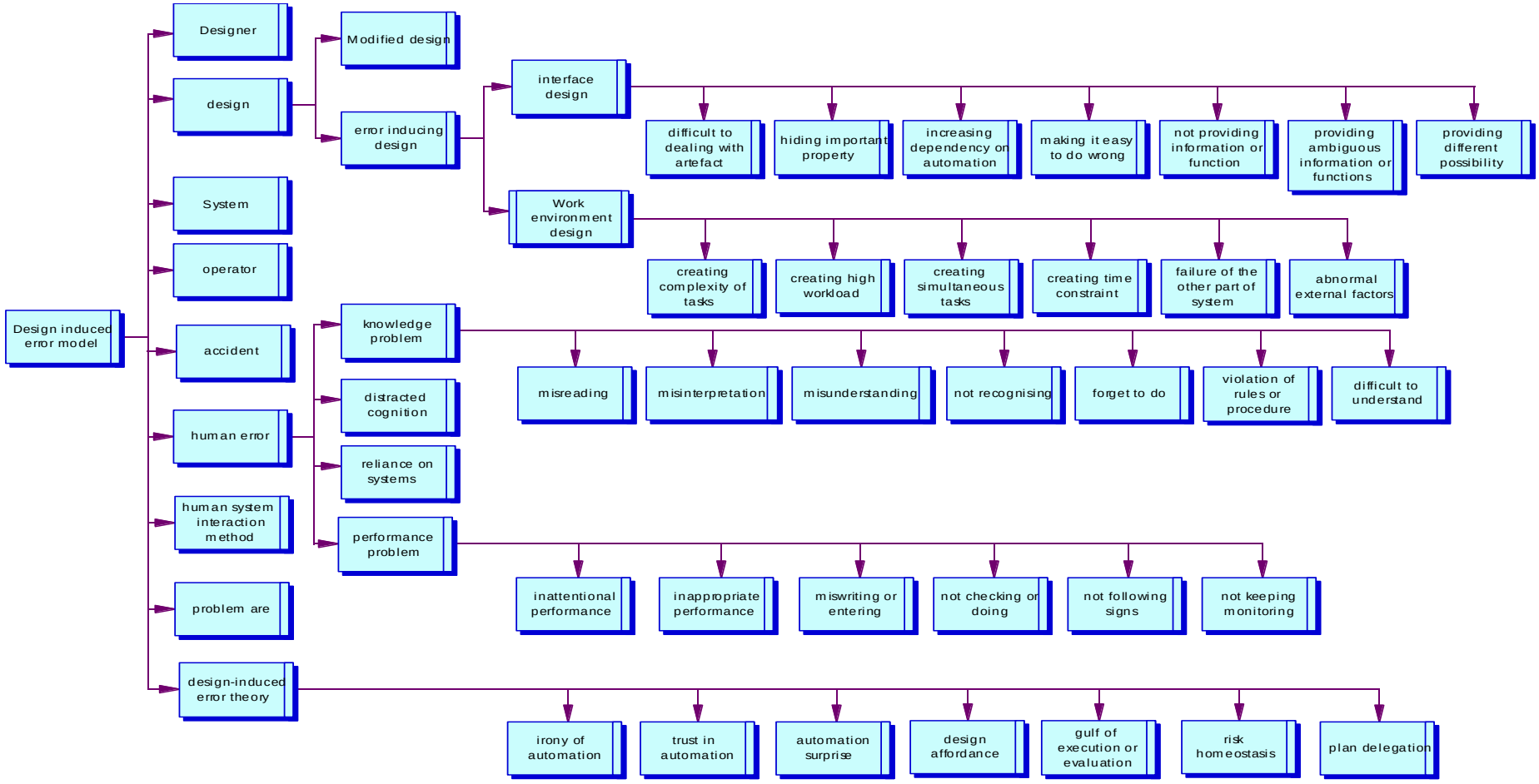


Figure 7.17 The concept tree of design-induced error

7.4.2 The error-inducing design ontology part

Error-inducing design ontology part is a part of design concept (Figure 7.18). The model of design-induced error ontology has two categories of design; “error-inducing design” and “modified design” in order to capture relevant information on design from accident report documents. The concept of “modified design” is to represent information if we find a description about a recommendation on a modification of design of a system that had design issues in the course of an accident investigation.

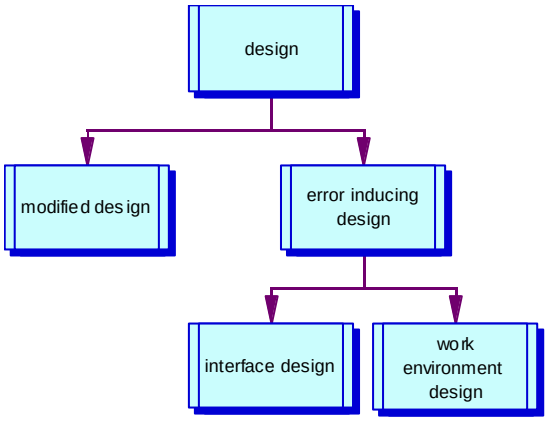


Figure 7.18 The classes of a design concept

The concept of “error-inducing design” has two sub-classes of “interface design” and “work environment design”.

According to the meta-theory of design-induced error, we can induce the following propositions:

Proposition 1: Design of a system creates “temporal decision making condition” in which operators have difficulties recognising problems dealing with a task by introducing simultaneous tasks.

Proposition 2: Design of complexity and automation creates ambiguous interaction between operators and systems.

From these propositions, the class of error-inducing design has two subclasses; “interface design”, and “work environment design”.

Low-level concepts of the two subclasses were determined by examining accident reports. The low-level concepts were classified in the light of searching relevant concepts in the text (Figure 7.19, Figure 7.20).

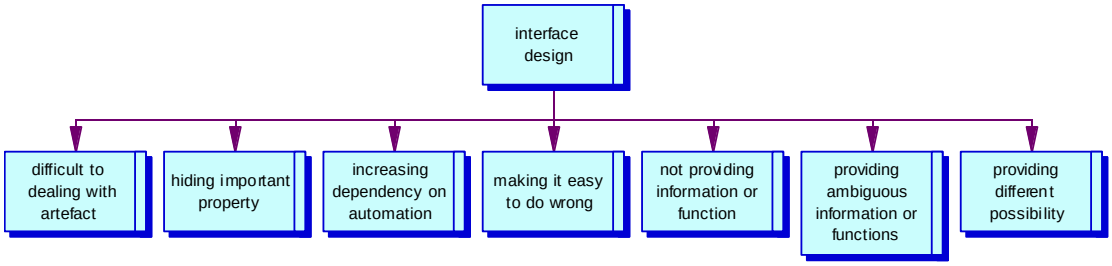


Figure 7.19 Sub-classes of an interface design concept

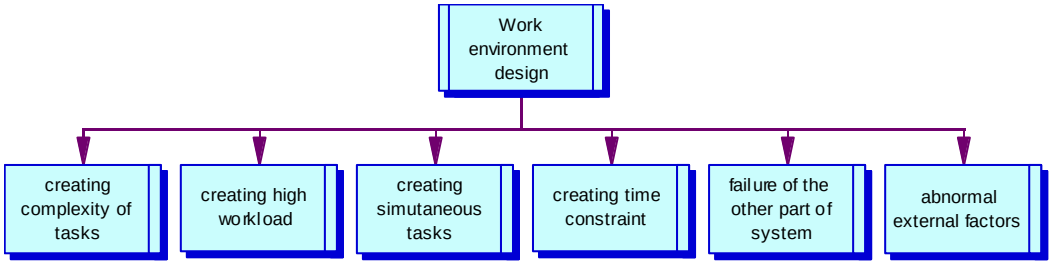


Figure 7.20 Sub-classes of a work environment design concept

The concept of error-inducing design has four relations with main concepts. It has an "is affected by" relation with the concept of operator, an "is explained by" relation with the concept of theory, an "is induced by" relation with the concept of human error, and an "is unsolved by" relation with the concept of problem area (Figure 7.21).

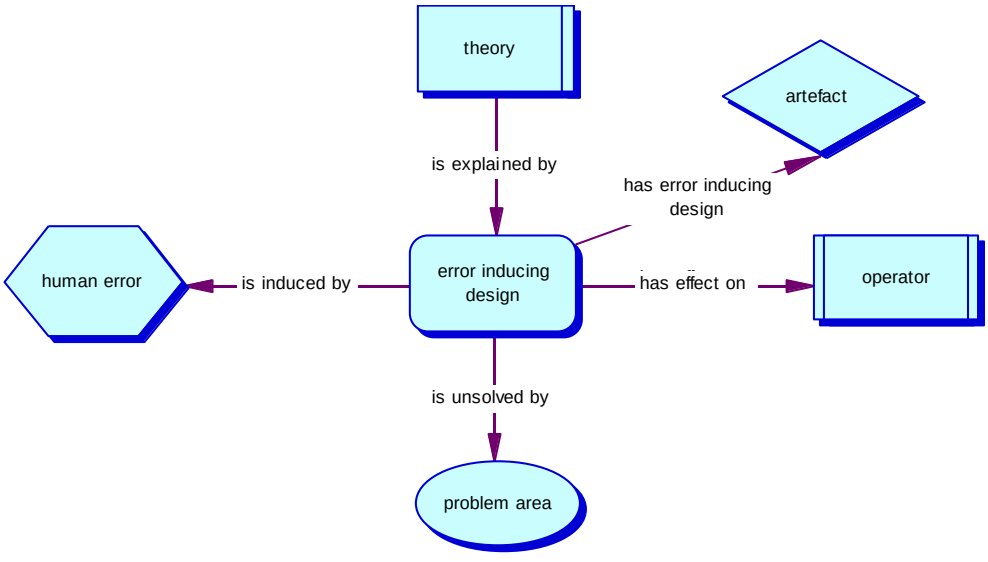


Figure 7.21 Relations of an error-inducing design concept

7.4.3 The human-error ontology part

This is not a pure psychological classification of human error. The concept of human error in this thesis is categorised by four sub-classes. Each sub-class represents parts of the descriptions in accident reports. For example, a description of "the pilot in command was distracted with other tasks…" in an accident report is captured in the category of "distracted cognition" (Figure 7.22).

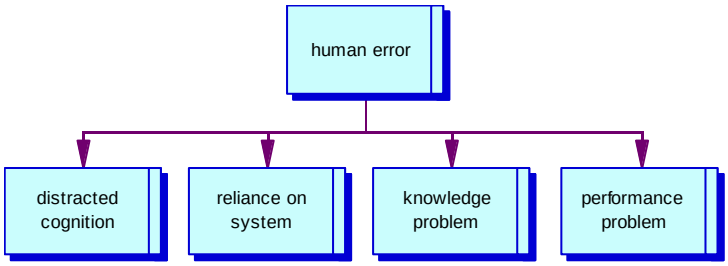


Figure 7.22 Sub-classes of a human-error concept

The concepts of "knowledge problem" and "performance problem" occur in a lot of forms of human error. They have several low-level classes that represent part of failures of human operators. The concept of knowledge problem encompasses mainly perceptual errors of operators (Figure 7.23), while the concept of performance problem captures activities of the operators (Figure 7.24). They are not comparative concepts because they can appear together in the same document.

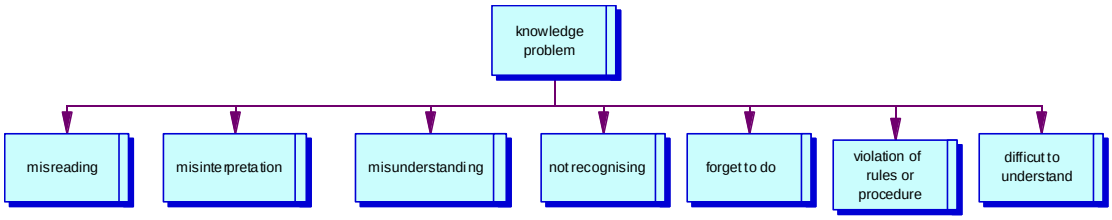


Figure 7.23 Sub-classes of a knowledge-problem concept

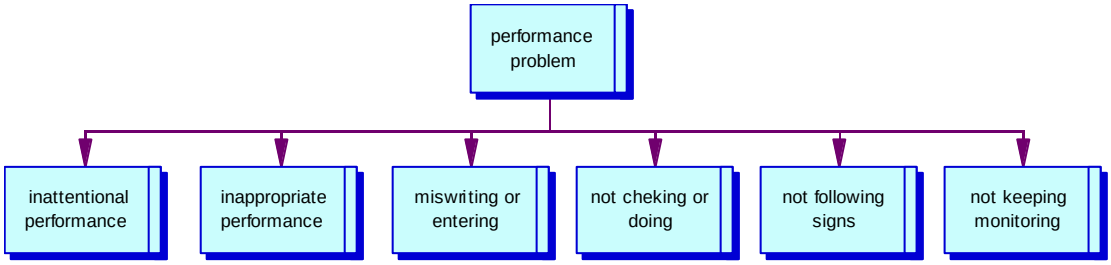


Figure 7.24 Sub-classes of a performance-problem concept

Relations in the concept of human error have several links. It causes an accident with "has cause" relation. Other relations are shown in Figure 7.25.

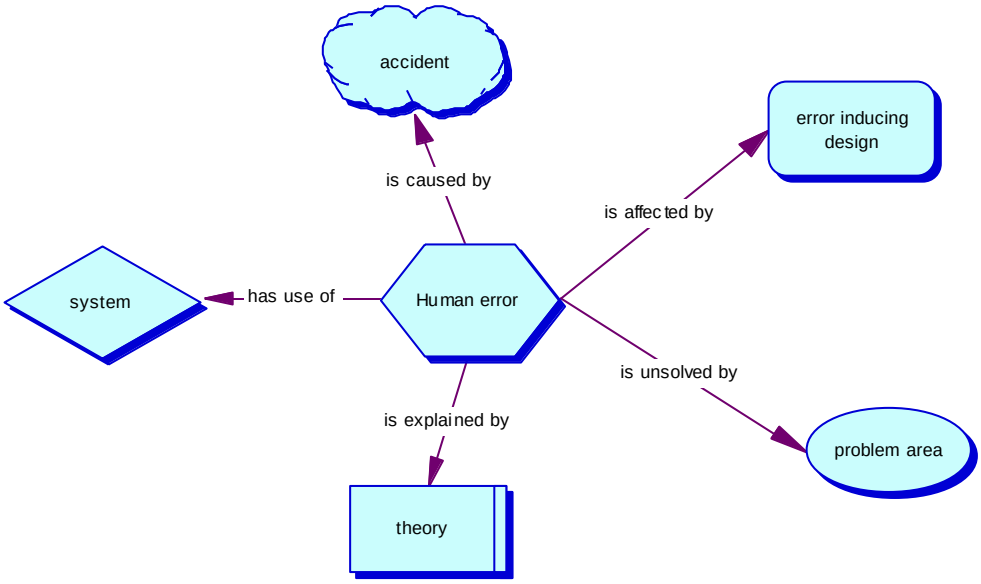


Figure 7.25 Relations of a human error concept

7.4.4 The design-induced error theory ontology part

There are seven theories to represent the concept of design-induced error (Figure 7.26). The ontology has a concept of "design-induced error theory".

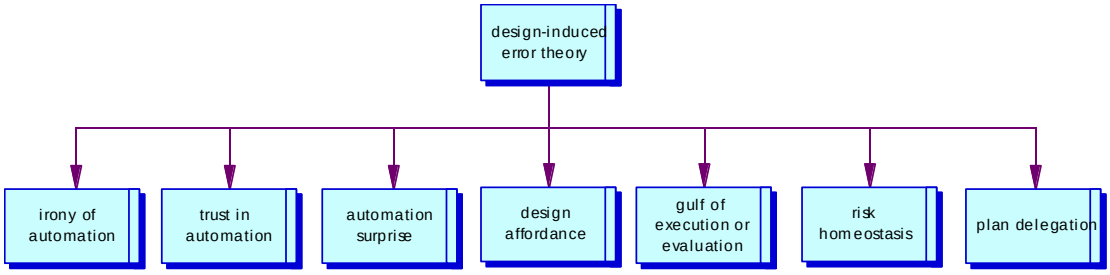


Figure 7.26 Sub-classes of a design-induced error theory concept

Theory has a relation of "has explanation of" with a concept of "human error" and "error- inducing design" (Figure 7.27).

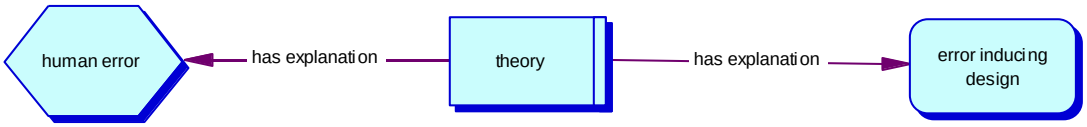


Figure 7.27 Relations of a design-induced error theory concept

7.5 Summary

This chapter developed a theory-based ontology of design-induced error. The idea at first to hypothesise a "*meta-theory of design-induced error*" that addresses relations between human error and design (see in Chapter 4) was used in this thesis in order to be used as a theoretical basis of interpreting human–system interaction failures. The meta-theory of design-induced error explains phenomena with which some design characteristics provide human operators with false recognition of the system in various ways, resulting in errors. According to the meta-theory, design and human error have relations between them but it is difficult to notice the relationship in real contexts because their relations are indirect and weak. This means that the interpretation of functions and features of the artefact or system that affect human cognition and performance need to be more clearly described.

It is argued that if we can draw the relations more clearly than before, even if they are weak links, it will help designers to understand and reason about human–system interaction failures. From this point of view, the concept of design-induced error therefore is not only a definition of a particular error form but also refers to a methodology to find weak links between design and errors for a knowledge-capturing purpose. With this point of view of the concept of design-induced error, this research demonstrated relationships produced by the ontology that show relations between

human error and design captured in real accident cases. These relationships also depicted relations between design issues and errors with a visual form (i.e. SVG, scalable vector graphics diagrams).

This research especially tried to show that an ontology browser developed with a web-based annotation tool can be used for searching for and understanding a particular knowledge effectively instead of just reading and reasoning on the contents of texts, which inevitably takes a large amount of time and effort in order to understand the knowledge in current documentary systems.

It is believed that the outcome of this research can be used for further development of methodologies to understand underlying meanings in unstructured text-based web documentation. For example, although accident reports, which were used in this study, may have a large quantity of information, it is still difficult to extract relevant knowledge automatically from the reports because the report is composed in the form of natural language. The ontology developed in this research can be used for tackling such a problem with the natural language processing (NLP) methodology and machine learning process.

It is hoped it can be also extended into developing a simulation technique of human–system interaction failures, which show people a visual demonstration of a failure, from accident reports. Those efforts may increase the usability of accident report documents for different approaches of accident analysis without damaging their original contents.

The next chapter will examine the developed ontology in terms of knowledge sharing: *Is this ontology useful for sharing knowledge of design-induced error (e.g. reasoning support, knowledge retrieval)?* It will then discuss related questions arising during development of the ontology.

Finally, it is necessary to mention about limitations of this research of ontology development: (1) It was not a detailed and complete constitution of ontology research but a prototype study for the subject of the research, i.e. in order to examine and demonstrate effective ways to capture and represent implicit psychological knowledge. (2) The area of developed ontology presented in this thesis was specific and limited to the Australian aviation accident incident reporting system. As a result, it is necessary to extend and modify the ontology further if one wanted to apply the ontology into another domain.

Chapter 8. Investigation of the developed ontology in the light of knowledge sharing

The previous chapters developed a theory-based ontology model of design-induced error. This chapter investigates what to do with the developed ontology (including the meta-theory). When we develop an ontology it is necessary to examine applications of the ontology according to the purpose of ontology development. The developed ontology has knowledge acquisition tools (e.g. a mark up template, annotation template, ladder tool) and knowledge modelling and representation tools (e.g. an ontology browser, diagram tool). Such features are expected to help users to capture relevant knowledge with connection of related concepts. The ontology developed should have an effective form and methodology to disseminate the concept of design-induced error. The investigation of developed ontology is therefore focused on the needs.

There will be a number of questions to investigate the design-induced error ontology. In general, the investigation issues in this research can be divided by three categories; a knowledge retrieval issue, a knowledge representation issue, and a reasoning support issue, because the purpose of the ontology is to deliver the knowledge of design-induced error to designers and to share the knowledge with them (Figure 8.1).

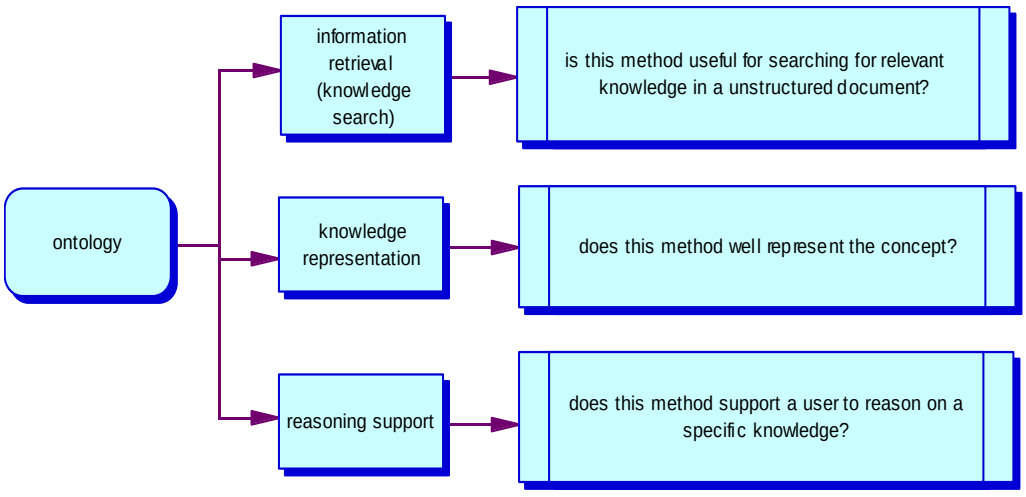


Figure 8.1 Investigation issues on the ontology developed

- Is it effective way of knowledge representation (KR) of the concept of design-induced error?

- How does the developed ontology help people to think about design issues in human error?

- Is it a better methodology of knowledge retrieval and acquisition than manual description analysis?

- Is there any possibility to extract related concepts in effective or automatically?

- Is there any recommendation for document structure for effective knowledge sharing of the concept of design-induced error?

This chapter begins with an evidence issue of design-induced error (Section 8.1). Evidence for a concept is important and the most fundamental issue is to search for the concept and related knowledge, and to validate ontology of a concept. The issue continues in section 8.2 of knowledge retrieval from accident reports. Several examinations were conducted for tackling the knowledge extraction issues. . A keyword search methods for DIE is examined in this section. Section 8.3 discuss the knowledge reasoning issues with the meta-theory application and propose two reasoning support tools for the concept of Design-induced error. These sections review how the method developed could be applied to finding design issues in accident cases. The issue about how well the developed ontology represents a concept of Design-induced error, i.e. a knowledge representation issue, is investigated in the Section 8.4. Section 8.5 expresses the usefulness of knowledge acquisition in the PCPACK ontology tool. Finally section 8.6 summarises the investigations.

8.1 Evidence issue

In the course of the research two different viewpoints on the concept of design-induced error were discussed. One comes from a psychological point of view and the other from a knowledge engineering point of view.

The former viewpoint argues that the concept of design-induced error can be used for reasoning about human error cases. This view focuses on how to apply the concept to understand human–system failures more than on what kinds of characteristics the

concept has. For this purpose, it is not a main task to clarify characteristics or to prove the concept (a meta-theory) because theories that conceive the concept of design-induced error have been proved in the previous researches. A meta-theory does not create any new theory that needs to be proved. The concept provides a possibility of the interpretation of design-induced error in any human error cases if there are system and human–system interaction failures unless other factors are found that affect the failure.

The latter needs countable evidences that show a concept of design-induced error. From this stand of application it is not reliable and realistic to recognise the concept in knowledge-based systems, if there is no physical evidence in an accident report to show the concept. As a result, the knowledge associated to the concept could not sharable between users in the system.

However, both approaches are at the same time useful and necessary to understand a concept of design-induced error. The former help to develop a meta-theoretical methodology of reasoning on design issues in human error. A psychological approach adopts such a view. The discussion in chapter 4 contributed in this case. The next section discusses the issue. The latter helps to formulate the ontology of the concept that represents the concept, and to search for the concept in knowledge-based systems. This is an important issue of ontology development (chapter 7). It is, in any case, important to investigate the evidences of a concept.

Questions arising for investigating an evidence discussion are:

1) How to support the concept of design-induced error?

2) What are characteristics of design-induced error?

If we focus on finding a particular type of human error in accident reports, we have to find evidences that show the error. Does a particular document describe characteristics of design-induced error or not? How to differentiate design-induced error from other errors? As mentioned in chapter 4, theoretically a distinction is assumed between the design-induced error and other errors depending on the fact that the error has different perspectives between the designer of the system and the operator in the system. This is a fundamental difficulty to differentiate design-induced error from other types because it is difficult to elicit such a different perspective without intensive investigation on the design concept of the system and the operator's perception of the system's operation. While conducting an analysis of accident reports, it was clear that there is no way to differentiate design-induced error forms from the other error forms. Error forms that describe an error are same (e.g. misinterpreting, mismanaging etc.). The fact that we can find any different error form between design-induced error and the other human

errors was verified during accident analysis of accident reports. For example, case 1 (O.N. 199902928) describes an operator error, "the pilot inadvertently moved both bleed air switches". However without reading other parts of the report, contextual circumstances surrounding the pilot at the time of making the error, such as a re-programming task of GPS and an instruction of ATC, we cannot say the error of the pilot was induced by the design of the system.

Therefore it is necessary to know the relationships between contextual factors and human error in order to identify design-induced error. They need to investigate intention of the design of a system and expectation of the operator involved in the accident. This is an intensive investigation task of investigators that is not normally conducted.

In spite of this difficulty it was found that parts of accident reports provide some evidence to show the concept of design-induced error. Based on the description of accident reports, evidence levels were categorised 5 scales (Table 8.1). Scale 5 and 4 has relatively strong evidence because expression in documents exactly matches with phenomena theory describes and accident investigators also mention design issues. Sometimes the reports described that a design has been modified after the accident.

SCALE OF EVIDENCE (STRENGTH)	SIMILARITY TO ISSUE STATEMENT	CRITERIA	RULE AND EXAMPLE
+5	Equivalent to issue statement	Report contains design problems with regard to human–system interaction and recommends modification of the design	Evidence level 4 + [design improvement]
+4	Equivalent to issue statement	Reports contains design problems with regard to human–system interaction	Evidence level 3 + [design issue]
+3	Similar to issue statement	Reports describe possible relationships between degraded operator's cognition or performance and design	Evidence level 1 + [may lead to error]
+2	Similar to issue statement	Reports describe breakdowns of relationships between operator's cognition or performance and system's activities	Evidence level 2 + [high work load]
+1	Analyst unsure	Reports do not clearly show the relationships, but theory supports possibility of the part of a concept of design-induced error if there is no other contributory factor.	[misperformance], [automatic response], [distracted], [unaware]
0(U*)	Analyst unsure	Reports express operator error without reason given for the error	[operator error]

* U : undefined

Table 8.1 Scale of evidences

Scale 3 and 2 has medium evidence because expression in documents roughly matches the phenomena theory describes but investigators did not clearly mention design issues. In case of scale 1 and 0, tt is difficult or impossible to judge design issues with human error from the expression in documents itself.

Result: From description analysis of accident reports from the Australian Aviation Accident Reports System, 287 human error accident cases were extracted for evidence analysis. These cases were classified into six levels of grade scales (5 to 0) according to above evidence levels of the concept of design-induced error. Table 8.2 shows evidence classification of accident cases that contain human error. It was found that the accident reports of below 2 on the scale of level of evidences are not useful for knowledge acquisition process due to lack of information. From this classification therefore, 52 cases out of 287 accident reports, above 3 scale (with grey background colour), were chosen as domain documents for use in the ontology development in the knowledge acquisition and modelling process.

Table 8.2 The result of classification of accident cases according to evidence levels (ATSB, 1995 –February 2005)

SCALE OF EVIDENCE	5	4	3	2	1	0
A NUMBER OF CASES	11	20	21	44	47	144

Discussion: This evidence searching process revealed some important characteristics of accident reports that must be considered in the process of ontology development.

(1) It is not possible to differentiate a design-induced error form from other human error without considering contextual environments during the process of an error.

(2) It is hard to extract clear and direct evidences of a concept of design-induced error from accident reports.

(3) Terminologies used in reports to express a similar situation or condition vary.

(4) Many reports lack information on design issues related to human error. It would be possible to capture such information if the accident investigation was conducted in more detail and was more concerned about the issue.

8.2 Investigation on a knowledge retrieval issue

Knowledge retrieval (i.e. information retrieval) is to extract information in a form of concept relation from a source. It means that knowledge retrieval is a methodology to search for a relevant information chain to an issue in data that is not predefined. For knowledge retrieval in unstructured documents, technology has developed several methodologies (e.g. text mining[Dörre et al., 1999; Hearst, 1999]) in order to extract knowledge from unstructured documents.

The primary methodology of knowledge retrieval is a key word type that has been used in many search engines. The other ways, such as a text-mining method or the Dempster-Shafer method, are based on statistical or Bayesian techniques that need a quantity of data.

In the knowledge elicitation process (chapter 7) it was revealed that the concept of design-induced error cannot be formulated with only one set of a concept. It needs relations between different concepts, i.e. human error and error-inducing design (Figure 8.2).

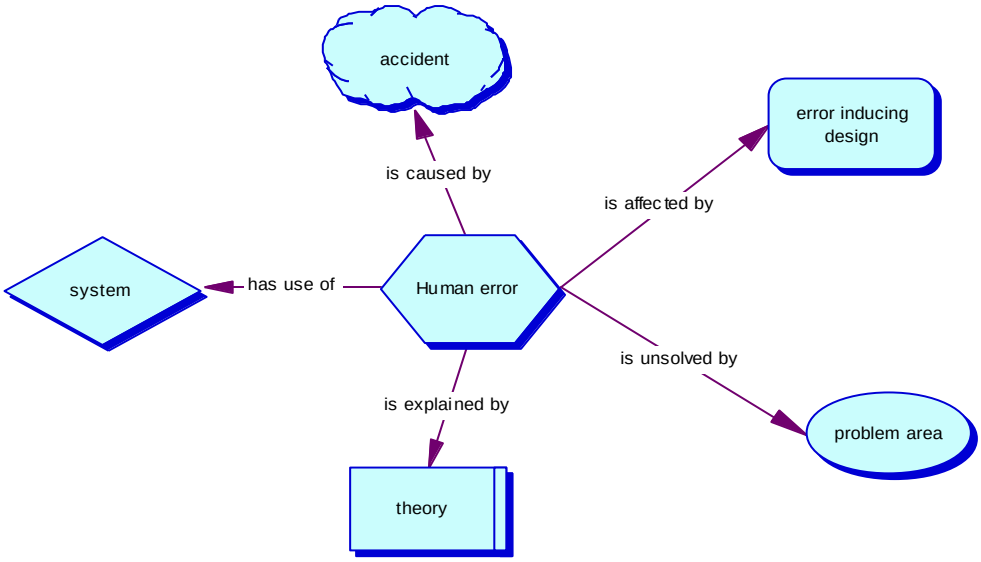


Figure 8.2 Human-error relations

There is no way of extracting the concept without a complicated process. Extracting material relevant to design-induced error from accident report documents cannot depend only on one method. Some files were examined and tested with different information retrieval methods (e.g. a text-mining method, Dampster-Shafter method). However these methods were not relevant to extract a concept of design-induced error

from the accident reports. Their methodologies depend on statistical relations between documents. In the case of the concept of design-induced error, the underlying meaning of expressions in a document is important. The number of items of good evidence of expression for the concept was low (as discussed in Section 8.1) resulting in making a statistical approach difficult. Therefore, text-mining methods (e.g. Tropes, QDA Miner software) were used only for analysing keywords. Through this examination, It was possible to define keywords in two concepts, i.e. human error and theory relating to design-induced error (Table 8.3, Table 8.4).

This process finds keywords or sentences that represent a human error. For example, the human error appears in a document in terms such as, "the pilot inadvertently moved both bleed air switches" in an accident case example (Figure 8.3).

Occurrence Number:	199902928
Occurrence Date:	21/06/99

The additional workload created by instructions from ATC, and from attempting to re-program the GPS at the time when he was completing his climb checks may have captured his attention, thereby reducing his capacity to notice deviations from normal procedure.

Normal procedures included re-positioning blower switches at this stage of the flight. These switches were located very near to the bleed air valve switches, and it is probable that the pilot inadvertently moved both bleed air switches to ENVIR OFF during the climb checks instead of moving the two blower switches. An inadvertent repositioning of the bleed air switches would not be detected by the sequenced monitoring of the pressurisation instrumentation in the climb checklist, as the pressurisation check was before the airconditioning and aft blower checks.

1. Both bleed air switches were inadvertently selected to ENVIR OFF at about 10,000 ft in the climb.
2. The cockpit warning system did not adequately alert the pilot to the cabin depressurisation.
3. The oxygen mask deployment doors were incorrectly orientated during installation, so that the masks would not automatically deploy when required.

4. Hypobaric training did not provide an effective defence to ensure that the pilot or passengers would identify the onset of hypoxia.

Figure 8.3 An example of accident reports description analysis (in ATSB, 1995 – February 2005)

Discussion: With a keyword-type approach we can categorise relevant keywords in rough. However, there is no one keyword for capturing the concept of design-indced error. Several terms are correlated each other. In order to extract the concept of design-induce error we need to identify relations between related terms.

Table 8.3 The category of keywords related to human error (ATSB, 1995 – February 2005)

DESCRIPTION CATEGORY	KEYWORDS
Defective cognition	Distracted, late decision, did not notice, without checking, assuming, unable to communicate effectively, did not get a response, incorrectly identified, misread, not been made aware, convinced, error of expectancy, not provide, false impression, did not see, neither crew being aware, unlikely considered, did not adequately monitor, confusion, their attention had been directed, no coordinated response, etc.
Performance problem	Should have alerted, did not advise, recorded incorrectly, did not conduct an effective scan, not appreciate, ignore, overlook, inadvertently steer, did not hear, incorrectly indicate, inadvertently select, did not change, the controller's scan was inadequate, without an effective alert, not appreciate the potential for conflict, incorrect display, initiated a missed approach, diverted from, poorly constructed, misinterpreted, etc.
Knowledge problem	Assume, did not appreciate, probably assumed, not adequately scan, did not provide, did not issue, not accurately judge, no assurance, did not recognise, not clearly defined, did not inform, did not appear to understand, developed incorrect mindset, without broadcasting, etc.
Distracted cognition	Distracted, diverted his attention, familiar with, never seen this approach, did not consult with, controller's recognition, assumption, assumed, considered, not familiar with, not in the practice, was rare, his decision was influenced by the fact, have been developed over several years, previous occasions, etc.
Reliance on systems	Rely on, considered unreliable, was confident, relied exclusively on, assumed, different expectation, incorrect estimate, relied solely on, over-reliance, this belief may have resulted in, was surprised by, surprised at, believed, was surprised when, dependent on, mislead, etc.

Table 8.4 The category of key words related to theories of design-induced error (ATSB, 1995~2.2005)

CATEGORY	KEY WORDS	CASES
Design Affordance	Inadvertent deletion, inadvertent selection, inadvertent failure, misread, inappropriate/inadvertent flap slat selection, displayed incorrectly	11
Gulf of execution/evaluation	Assume, misinterpret not display, was not provided, difficult to read, overlooked, misidentify, erroneous entry, difficult to distinguish, the chart was ambiguous, difficult to see, erroneous perception, unaware, misinterpret, misread, incorrect display, did not fully understand	43
Irony of automation	Not monitor, not notice, not recognise, inadequate scan, distracted, unaware, decision was inappropriate, diverted his attention, inadvertently selected wrong code, unable to detect, not notice, misplace, misinterpreted the data link, less vigilant in his monitoring, did not appreciate the potential conflict, inadvertently omitted, neither controller realised	15(inability) 46(monitoring failure)
Trust in automation	Believe, over-reliance, expect, incorrectly interpret, without warning, did not review	9
Automation surprise	Not understand, not recognise, surprise	1
Plan delegation	Forget, did not check, relied exclusively on, overlook, not recognise	11
Risk homeostasis	Rely on their interpretation, did not preclude, did not follow	9

8.2.1 A keyword search method for the human error and design issue document retrieval

Although it is not exact knowledge extraction methodology, a keyword type search method has still good merits such as easy and effective applicability for general users than other methods. This study tested an applicability of the keyword search method and discussed its limitations.

The keyword type information search method is not a semantic search method. However, it is a useful method to sort out accident reports in amount of document file into relevant cases (for example NTSB accident database system has 140,000 cases). While insufficient description evidences of human and design errors existing in accident reports, as a first step to developing automatic knowledge extraction methods, this will help to retrieve relevant cases of DIE reasoning from accident report systems.

I propose a method to extract relevant documents. The "relevant document" of DIE in this paper refers to a document that contains (1) human error and (2) relationships between the human error and activities or existence of systems or artefact. Such documents are called as "reference document of DIE" because we can refer the document for reasoning on design issues in human errors.

Reference documents have not only documents that contain exact cases of design-induced error, but also documents that have a possibility of design errors related to human error. It is important not to exclude useful documents for DIE reasoning analysis by analysts.

Retrieval Process

Step 1. Querying with combined terms between engineering related terms (i.e. system / artefact) and design-induced error theory related terms.

- Engineering related terms (e.g. "landing gear" or "autopilot") + design-induced error theory related terms (e.g. "inadvertently" or "rely")

Step 2. Sort out returned documents by eliminating irrelevant documents

- Eliminating documents clearly irrelevant cases that is not describe operators and systems or artefact (e.g. …he rely on God….)

Step 3. Analysing sorted cases with the related theories.

- Reasoning on design-induced error in the retrieved documents (why the operator at the time of the accident made errors? Is it possible to explain the error with design-induced error theories?)

Finding different perspectives of designers and operators in the case

8.2.1.1 An experiment of information retrieval for design-induced error reasoning.

This experiment examined two theories of design-induced error: a theory of design affordance and a theory of trust in automation. From preliminary analysis of accident reports in the Australian aviation accident report system, two keywords of the theories were taken and used for the information retrieval task.

· The term "inadvertently" for the design affordance theory

· The term "rely" for the trust in automation theory

Three accident report systems were examined for the experiment Table 8.5). NTSB has one of the largest aviation accident database system containing 140,000 accident cases.

Table 8.5 Accident report systems used for the experiment

ACCIDENT DATA BASE SYSTEM	NUMBER OF CASES IN THE DATABASE	PERIOD	RESOURCE
ATSB (Australian Transport Safety Bureau, http://www.atsb.gov.au/)	780	1994-	Aviation accident and incidents in Australian
ASN (Aviation Safety Net, http://aviation-safety.net/database)	12,200	1943-	Aviation accidents around world
NTSB (National Transportation Safety Board, http://www.ntsb.gov/ntsb)	140,00	1962-	Aviation accidents and incident in USA

As search engines the Google search engine and NTSB database query system were adopted.

· Google search engine

· Database Query system in the NTSB Accident Data & Synopses system

Query terms in Google search engine (examples):

- (relied OR rely OR relying) AND autopilot site:http://www.ntsb.gov/ntsb/
- "not detect" -mair -train -rair site:http://www.atsb.gov.au/publications/investigation_reports/
- human error site:http://aviation-safety.net/database/

8.2.1.2 Results

As the first test some keywords were put into the search engine system. Table 8.6 shows the results. The reason of different results between Google and NTSB search engines is that they may use different algorithms.

Table 8.6 show the result of terms "inadvertently", "rely".

Table 8.7 query results combined with a term "inadvertently" from the Google search engine (for design affordance theory).

Table 8.8 query results combined with a term "rely" from the Google search engine (for trust in automation theory)

Table 8.6 Query results from the Google search engine (10 June 2006)

Query terms	ATSB	NTSB	ASN
Inadvertent(ly)	77	67,000 (2,820)*	302
Rely(ied, ing)	66	138 (134)	29
Design	203	17,700(1,562)	316
Design AND inadvertent(ly)	20	113 (47)	17
Design AND rely(ied)	17	7 (30)	-
Pilot failure	1	69,800 (more than 5,000 returns**)	146
Pilot failure AND inadvertently	-	847 (778)	15
Pilot failure AND rely	-	6 (-)	-
Error	83	645 (308)	596
Error AND inadvertently	17	24 (20)	1
Error AND rely	19	6 (6)	-
Human error	28	10 (6)	31

*( ) results from the NTSB database system query returns

** returns are too many, the system can not display all retrieval (the NTSB system display is being limited to the first 5000 records)

Table 8.7 Query results combined with a term "inadvertently" from the Google search engine (for design affordance theory)

COMBINED TERMS	ATSB	NTSB	ASN
Without combined terms	77	67,200 (2,820)	302
Control	64	21,400 (1,090)	113
Autopilot	19	46 (31)	29
System(s)	59	26,200 (335)	77
Landing gear	31	972 (355)	38
Computer(s)	15	32 (30)	-
Display	23	55 (91)	1
Flap(s)	29	794 (281)	41
Throttle	11	356 (154)	22
Trim	19	142 (91)	15
Switch(es)	24	327 (205)	17
Gauge(s)	11	70 (46)	-
GPS	12	42 (34)	1
Select(ed, ion)	42	297 (245)	27
Similar(ly)	36	95 (66)	-
Retract(ed, ion)	17	11,300 (266)	28
Stall(ed)	18	29,400 (1,772)	79

Table 8.8. Query results combined with a term "rely" from the Google search engine (for trust in automation theory)

Combined terms	ATSB	NTSB	ASN
Without combined terms	66	140 (134)	29
Gauge(s)	9	44 (36)	-
Autopilot	10	9 (9)	1
System(s)	51	75 (59)	-
Instrument(s)	37	63 (50)	14
Computer(s)	11	6 (8)	-
Display	22	2 (20)	-
GPS	12	10 (10)	-

The return results of the query were screened. For example, in the theory of trust in automation the query term "rely" returned 138 cases in NTSB in the Google search.

After screening irrelevant documents manually from retrieved documents, 59 relevant documents were identified as matching with the concept. Precision of relevant documents was calculated (**Table 8.9**).

Table 8.9. Precision of retrieved documents for design-induced error according to terms

TERM	RETURN	MATCHING	PRECISION
"rely"	138	59	0.42
+display	2	2	1.0
+autopilot	9	7	0.77
+computer	6	3	0.5
+gauge	44	37	0.84
+system	74	35	0.47
+GPS	10	4	0.4

Precision is a percentage of number of reference documents in retrieved documents/ number of all retrieved documents. However, it should be mentioned that the precision in this study is exact precision of DIE because not all reference documents are exact cases of DIE. We cannot determine recall (number of relevant documents in retrieved document/ number of all relevant documents) because it is impossible that the number of all relevant documents. However, from the preliminary experiment at the Australian aviation accident report system this approach retrieves most of cases identified by the manual description analysis.

One interesting result from this retrieval is that many of cases of related to the term "gauge" were found in the search. The finding shows that pilots have heavily relied on gauge in a cockpit display. The theory of trust in automation has not told about artefact that is not directly related to automation systems. This result may imply we need to study this issue with the concept of design-induced error, and to expand current theories into these cases or to develop a new theory.

8.2.1.3 Limitation

This approach (i.e. reference document search) has a merit to include documents relevant to DIE reasoning as many as we can. However, its drawback is inaccuracy of retrieved documents searching for exact cases. This method still suffers from the inaccuracy retrieval issue. In order to increase accuracy we need methods to scrutinise returned documents. Main problems in this method are two: firstly, how to overcome diversity of expression of related concepts, and secondly how to define relationships between them. Machine has to understand the higher level of meaning of lexicon and their relations.

8.2.2 The proposed approach to DIE extraction

The proposed approach uses semantic annotations that annotate the reports with pre-defined semantics. The semantics are the defined concepts and relations in the ontology developed for this research. An ontology is an explicit specification of a conceptualization [Gruber, 1995]. The conceptualization is to give explicit definitions to domain concepts and their relationships using shared vocabularies. It is well known that the ontology improves information sharing and reuse [Noy and McGuinness, 2003]. In our research, the ontology is concerned with extracting information from unstructured texts, e.g. accident reports. In addition, the ontology supports to organize the DIE concepts into a hierarchy.

8.2.2.1 DIE ontology

The ontology development involved defining DIE related concepts and their hierarchical organization and their inter-relationships. The ontology has a capability to express the meaning above in related concepts and relations. Concepts in the ontology of DIE are entities that are needed to identify DIE such as HumanError, HumanErrorInducingDesign, Artefact etc (Figure 8.4). Relationships are essential for expressing the concept of DIE by connecting related concepts e.g. HasError, HasExplanation etc. Chapter 7 describe the ontology development in detail.

8.2.2.2 Annotation scheme

Figure 8.4 shows an example of using the annotations to identify the DIE concepts. That is, with the annotations we can easily identify a relationship between design and human error. For example, it is noticed that different types of design (e.g. operation methods, positions of switches etc.) in the fuel system induced the pilot in accident causing errors.

However, adding annotations manually is a time consuming and error-prone task, and more over, it is difficult to reuse the annotations across domains. This research is closely related to the application of an ontology-based semantic annotation within the Semantic Web (SW). The idea of the SW is to interpret information instead of just ranking it according to its popularity, the approach popularized by current search engines.

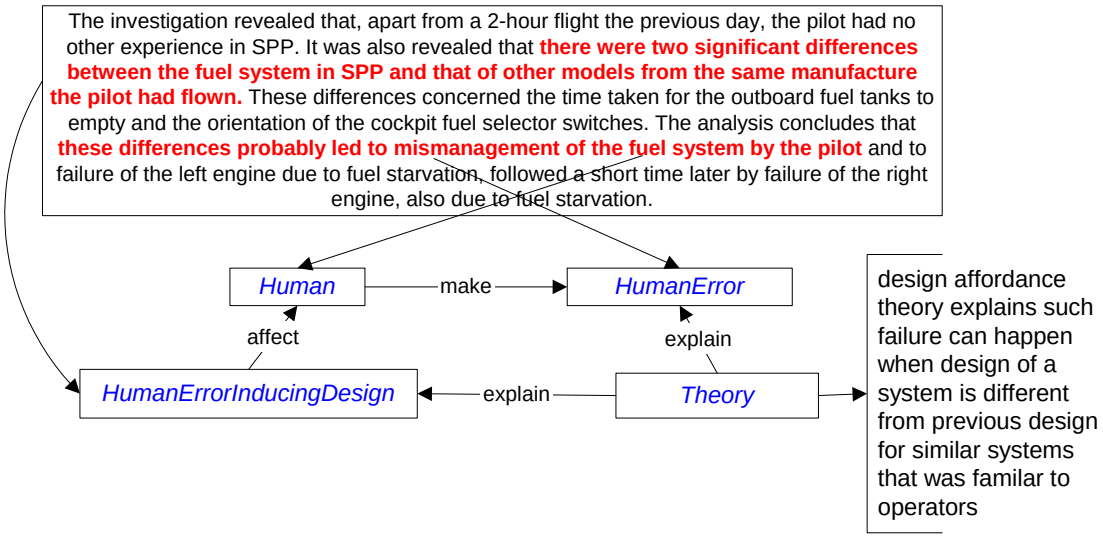


Figure 8.4 An example of the relations among four main entities

The Artequakt project [Kim et al., 2002] focused on generating dynamic biographies of artists using the information harvested from the Web. The biographies were then rendered according to user preferences using one of a number of pre-defined templates [Kim et al., 2002]. Rodrigo et al. [2005] created a search engine that exploited ontological knowledge in answering users' natural language queries that looked for specific information instead of whole documents.

Both systems used the techniques of Natural Language Processing (NLP) especially Information Extraction (IE) method for extracting information from the Web pages. IE performs well in extracting domain objects, e.g. people names, locations, product names, and their attributes using shallow lexical-syntactic patterns. However, since the potential influence of design weaknesses on fatal accidents is mostly described implicitly or ambiguously, the IE method might not be suitable for extracting such descriptions.

Instead, using certain cue phrases is helpful when it is hard to find regular patterns that constrain the occurrences of domain objects. Abdalla and Teufel [2006] proposed an approach that incrementally enriched cue phrases with variants. The cue phrases tested were pairs of transitive verbs and objects, e.g. introduce and method. While the method demonstrated high accuracy, it is not suitable for our task: although the pairs of verb and object are useful, other types of cue phrases, i.e. nouns (or noun phrases), or verbs without objects, are included in our case. In addition, our cue phrases can occur either within a single sentence or across sentences, in contrast to the cue phrases that Abdalla and Teufel tested which were only applicable to a single sentence.

The author is interested in cue phrases consisting of single word or phrases having some semantics that indicate certain types of sentences. For example, by identifying the phrase “did not notice” in a sentence, it may be feasible to assign the “recognition error” category as a type of “human error”.

Whereas these phrases clearly act as linguistic markers, because of syntactic and semantic variations, without checking, relying on cue phrases only can lead to low coverage and ambiguity. For example, it is difficult to identify a sentence containing “did not notice” as NOT being relevant to design error simply by looking up the cue. That is, it is necessary to define the context under which a cue phrases is not applicable. To address these limitations, we refer to the ontology definitions, especially by using the ontology triples, which allow incorrect detections to be filtered out by constraining which entities should be associated with specific relations.

That is, three elements found as necessary to direct correct identifications are: (1) the existence of cue phrases, (2) the relations defined in the ontology, and (3) relations between human and design induced errors described in texts.

This thesis proposes “evidential sentences of DIE” that contain cue phrases of DIE related concepts (see italicized phrases in Table 8.10). Our hypothesis is that an ontology based cue phrase method can help to identify relevant knowledge. We argue if we can extract related sentences it will help to understand related knowledge.

Evidential sentences are classified according to the concepts defined in the ontology. Two evidential sentence term category schemes are used in order to find design issues related to human error: Human error and Error inducing design. This classification may be expanded into subclasses as follows.

Human error category has following subclasses:

- Distracted cognition (DC)

- Reliance on system (RS)

- Performance error (PE)

- Recognition error (RE)

Human error inducing design category has:

- Human-system interaction design issue (HIDI)

- Work environment design issue (WDI)

- Modification of current design (MD)

8.2.2.3 Dataset and methodology

Dataset: The ATSB reports were selected for this research as described in detail in chapter 7. Methodology: For the ontology development the PCPACK tool kit was used. PCPACK provides protocol tools for annotating the reports with the concepts and relations according to the DIE ontology, a diagram and ladder tool for ontology modeling, and a publishing tool for viewing the annotated reports [Shadnolt and Milton, 1999].

8.2.2.4 Results

Semantic meaning is connected with rhetorical aspects of documents. The corpus of 52 accident reports that were selected from the ATSB system was a difficult test bed because they were identified by hand.

334 evidential sentences were extracted from the corpus manually. Table 8.10 shows some examples of extracted evidential sentences. It is small set but useful to develop a method to identify human error and its relation to design issues.

The annotation work was conducted with the PCPACK Protocol tool kit that makes it possible to mark up text by highlighting the text. Figure 7.13 show an internally published web page developed using the Ontology. Users can browse related concepts by clicking annotated concepts. This browser provides relations between potential design errors and human errors.

8.2.2.5 Discussion

This study discussed the issue of supporting engineering designers in accessing aviation accident reports especially for accidents caused by operators when interacting with the equipment in aircraft systems. Incomplete designs or differing perspectives between designers and the users with respect to the way in which the aircraft are used can contribute to the accidents. A main focus was to identify and extract the concepts related to human and design errors from the texts, and map the concepts to psychological theories.

Manually collected evidential sentence and cue phrases were used to discover extraction patterns and the patterns were further constrained by referring to the ontology definitions.

However, this is not an automated annotation work, as mentioned in previous sections manual annotations are an error prone and time consuming task, automatic annotation will be more effective and useful tool for capturing knowledge from documents. Therefore future works will be focused on developing automated annotation methods.

In order to develop such methods we have to overcome diversity of expression in concepts and to develop machine understandable grammars.

Table 8.10 Examples of evidential sentences

Distracted Cognition (DC):
-This aspect in conjunction with his operation of the controller pilot datalink probably caused the sector controller *to be distracted to the extent* that he was unable to maintain an adequate scan of the flight progress strips. (ATSB, 199802755)
Reliance on system (RS):
-The use of Operational Data Information for coordination between units was accepted as a standard operating procedure. On some occasions the overuse and *over reliance on Operational Data Information coordination* may lead to lack of situational awareness. (ATSB, 199900192)
Performance error (PE):
-The possibility of this occurring had been recognised by management and the instructions were issued in an endeavour to prevent *inadvertent deletion of a flight data record*. (ATSB, 199805341)
Recognition error (RE):
-Both pilots reported that they *incorrectly identified* the morse-code ICN signal on frequency 109.5 MHz as ICS, the morse-code identifier for the runway 15 ILS on frequency 109.9 MHz.(ATSB, 199902874)
Human-system interaction design issue (HIDI):
-The air traffic control strip printing system *did not provide for* a specific manoeuvring segment. (ATSB, 199702620)
Work environment design issue (WDI):
- The pilot reported that *he had then become occupied with re-programming* the aircraft's Global Positioning System (GPS). (ATSB, 200105188)
Modification of current design (MD):
-As a result of the investigation, the company operating the A320 *has amended* its flight-planning process by *making a modification to* the flight-planning system. (ATSB, 199702620)

8.3 Investigation on reasoning support issue

8.3.1 a meta-theory application issue

As conducted in Chapter 5 V^2 analysis presented a way how to capture design issues in human error cases. From the meta-theoretical point of view, a meta-theory of design-induced error can be used for recognising design issues in human–system interaction failure cases. This approach is expected to have an ability to support designers by providing an effective tool to show design issues related to human error in terms of design-induced error. In order to apply the meta-theory of design-induced error into analysis of human–system interaction failure, an analysis method below is proposed in this section.

Method: Analyse according to following procedure and record on an analysis sheet (Figure 8.6). V^2 analysis also combines with the process in order to find vulnerability of design and error modes. Figure 8.5 shows the process.

(1) Find human error cases in the accident reports

(2) Define human–system interaction failures

(3) Examine design purpose of a failed system (perspective of designers)

(4) Examine reason of human errors (perspective of operators)

(5) Extract design-induced error by comparing different perspectives of designers (step 3) and operators (step 4)

(6) Test related theories that match with meanings that arise in the previous steps

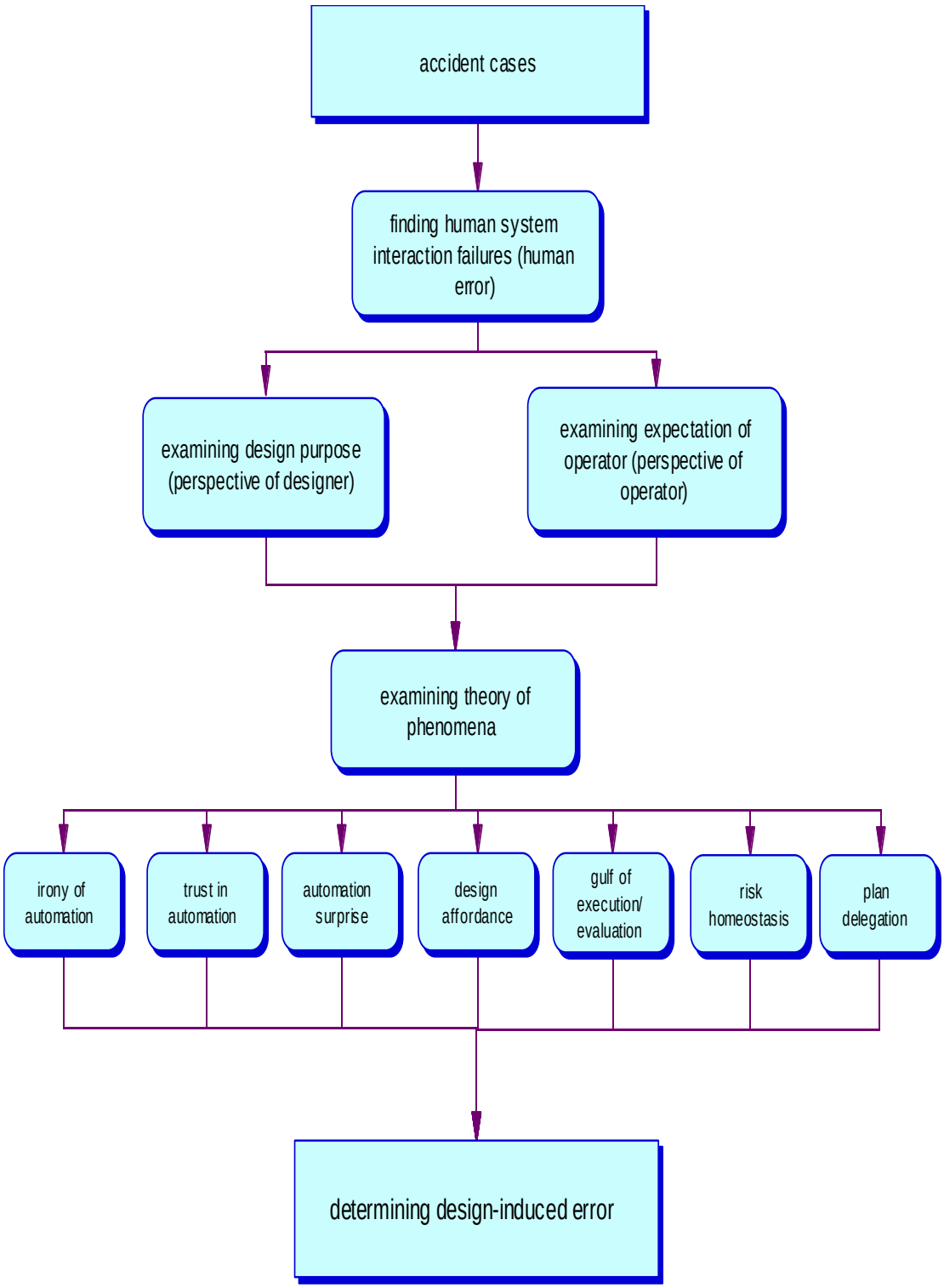


Figure 8.5 A reasoning process of the design-induced error model

Case number	
Accident description	
Human–system interaction failure	
Perspective of the designer	
Perspective of the operator	
Design-induced error	
Related theories	

Figure 8.6 An analysis sheet of human–system interaction failures in terms of design-induced error

Application of the developed meta-theory of design-induced error was conducted with data from the Australian aviation accident/incident report system. Two kinds of study of application of meta-theory were conducted: (1) clear cases of a design-induced error (according to evidence levels defined in the previous section), and (2) purely human error cases. Case studies conducted using the developed method are appended to this thesis.

8.3.1.1 Study 1: cases with good evidence of design-induced error

The cases taken from accident reports with good evidence of design-induced error i.e. scale of evidence 5 were examined. These cases were analysed according to the design-induced error analysis method (Figure 8.5) using the accident analysis sheet (Figure 8.6).

The following five cases are examples of high-evidence cases analysed in terms of design-induced error. From this methodology it is expected that we can gain a more clear understanding of different perspectives between designers and operators.

Case number	1				
Date of occurrence	21/06/99	Source	ATSB	**Occurrence number**	199902928
Accident description					
Accident system: Beech 200 Super King Air aircraft/ depressurising alert system/ vent blower switches selection procedure Progress: After take-off, as the aircraft climbed through 10,400 ft, the pilot began the 'climb checklist' actions. While performing these checks he received a tracking change instruction from Air Traffic Control (ATC). The passenger in the co-pilot seat noticed that this appeared to temporarily distract the pilot from the checklist as he attempted to reprogram the global positioning system (GPS). The pilot then completed the checklist. During this, the passenger in the co-pilot's seat saw the pilot reposition the engine bleed air switches from the top to the centre positions. As the aircraft reached the cruise level of FL250, the controller contacted the pilot, indicating that the aircraft was not maintaining the assigned track. The pilot acknowledged this transmission. A short time later the passenger in the co-pilot seat noticed that the pilot was again attempting to program the GPS, and was repeatedly performing the same task. The controller advised the pilot again that the aircraft was still off track, however the pilot did not reply to this transmission. Shortly after this, the pilot lost consciousness. The passenger in the co-pilot seat took control of the aircraft and commenced an emergency descent.					
Human–system interaction failure					
• The pilot did not notice the illumination of the depressurising alert. • The pilot inadvertently selected bleed air switches instead of the nearby vent blower switches. • The pilot did not finish after-takeoff checklist tasks (e.g. GPS setting) before entering a critical flight level.					
Perspective of the designer					
• Pilots have an ability to do tasks as scheduled in the design. • Pilots will check the position of switches correctly. • The more the automatic system, the more operators wll be helped. • Operators would be alerted by illumination of the warning system.					
Perspective of the operator					
• If there is a something to do urgently during a procedure, the attention of an operator should be focused on the task. • The array of switches would be arrayed according to the user's intention. • While conducting an important task, it is difficult to recognise other issues. The system should help. • The system should alert operators in an effective way.					
Design-induced error					
• As design of the procedure increased after-take-off checklists (e.g. GPS setting), the complexity and time constraints make it possible for a flight to climb automatically into a critical flight level. • The increased complexity distracted operators from checking other tasks, resulting in skill-based level of performances.					

• The close position of bleed-air switches and blower switches may lead the pilot to inadvertently moving the bleed-air switches to off. • Illumination of a warning system may not effectively alert people in the cabin to recognise depressurising problem before the pilot in command loses consciousness because there are a number of items of information to be checked in a cockpit display.
Related theories
Gulf of evaluation, design affordance

Case number	2				
Date of occurrence	03/05/99	Source	ATSB	**Occurrence number**	199902003
Accident description					
Accident system: ATC air traffic computer, VH-CZC (had taxied for departure), VH-TJW (had taxied after CZC, also for a departure from runway 15) Progress: Both crews had been cleared via the runway 15 SWIFT 2 standard instrument departure. After issuing the departure clearances, the controller commenced the process of making the change in the air traffic computer; an action that required nine clicks of the mouse. In order to make this change, the controller looked away from the air situation display (which was on the main screen) and used the auxiliary screen to observe the flight plan window while using the keyboard to input the data. While the controller was performing the information change task, the crews of the departing aircraft contacted him as required. The controller acknowledged the radio broadcasts then returned to the data input task. He did not continue to check the positional information on the air situation display. A few moments later, he glanced at the display and realised that TJW had turned earlier than CZC and was also out-climbing that aircraft. The vertical separation standard of 1,000 ft had not been achieved at the time. The controller immediately cancelled the standard instrument departure for TJW. Both crews subsequently reported that they received a traffic alert and collision avoidance system (TCAS) advice.					
Human–system interaction failure					
Controllers considered that the aircraft were "like types" for the purposes of departure standards and neither the aerodrome controller nor the approach/departures controller considered increasing the separation requirements specified in Local Instructions. However, the performance of the B737-400 series aircraft was superior to that of the B737-300 series aircraft. The use of minimum departure separation standards was inappropriate. The approach/departures controller elected to input data to the air traffic computer during the departure sequence.					
Perspective of the designer					
• The controller will verify the minimum departure standard design before confirming the procedure. • The controller will recognise different performance abilities between B737-300 series and B737-400 series. • The controller will check progress by keeping monitoring the relevant instruments. • The data entering work is not the main task but one of the sub-tasks and the sub-tasks do not affect the execution of the main task. • The controller will easily update traffic information after finishing a main task.					
Perspective of the operator					
• Similar types of aircraft have similar performance ability. • Progress of the departure procedure will be developed as designed so that it will be possible to conduct the data entering work during the development.					

• While conducting the data-entering job, the controller cannot concentrate on monitoring traffic situation.
Design-induced error
• In busy traffic conditions, it is a time consuming task to verify pre-designed departure standards. • There was no specific design to recognise different performance of similar types of aircraft. • There is no reserved schedule or designed procedure for the data-entering task only. The data-entering task is one of mandatory tasks, however, it is labour intensive and diverted the controller's attention from the air situation display.
Related theories
Irony of automation – Monitoring failure

Case number	3				
Date of occurrence	05/12/01	Source	ATSB	**Occurrence number**	200105715
Accident description					
Accident system: a Saab 340B Progress: While on climb through FL180, the copilot's two electronic flight information system (EFIS) screens on the right side of the aircraft's instrument panel failed. After the crew had consulted the EFIS failure/disturbances checklist, the central warning panel ice protection annunciator and then the cabin pressure annunciator illuminated. An emergency descent was initiated and the crew broadcast a PAN call to Air Traffic Services (ATS) and reported that they were returning to Trepell. During the descent a number of other cockpit warnings and cautions activated and some aircraft systems failed. The crew became aware that the right DC electrical generation system was operating abnormally. Their attempts to rectify that situation were unsuccessful. The crew diverted the aircraft to Cloncurry and landed.					
Human−system interaction failure					
The crew overlooked the first item of the EFIS failure/disturbances checklist, which required a check of the generator voltage.					
Perspective of the designer					
• The pilot will check the emergency checklist according to the order designed.					
Perspective of the operator					
• There will be a warning sign if a generator failed. • During emergency checks the pilot focuses on specific reasons of the screen failure at first in the EFIS checklist, not general issues such as a generator failure. • Generator failure is a too general a problem to recognise. As a result, if the generator failed, it is reasonable the other parts of system also failed.					
Design-induced error					
• There was no generator failure warning sign. In case of a failure of the EFIS screens, the emergency checklist was designed in order from generic checks to specific checks. In some Saab 340 aircraft a starter generator could fail without taking the generator off line and alerting the crew, resulting in low system voltage. • On this occasion it is easy for the crew to overlook the first item of the EFIS failure/disturbances checklist, which required a check of the generator voltage. Consequently, the crew did not recognise the developing low voltage condition that led to the cascading series of warnings, cautions and failures.					
Related theories					
Gulf of evaluation, Design Affordance					

Case number	4				
Date of occurrence	20/08/97	Source	ATSB	**Occurrence number**	199702691
Accident description					
Accident system: Bangkok Area Control Centre (BKK ACC) Sector 3 Progress: QFI6, a Boeing 747, had departed Bangkok for Melbourne and was tracking southbound on airway G463 at flight level (FL) 290. The aircraft was in contact with Bangkok Area Control Centre (BKK ACC) Sector 3. Sector 3 was a combined radar and procedural control sector. At 0212:54 QF16 reported passing ALGOR at FL290, estimating KABAS, the flight information region (FIR) boundary, at 0221. Just prior to reaching KABAS, the aircraft would pass the intersection of G463 and B219 at KATKI. These positions were all located beyond radar coverage, over international waters, within the procedural control portion of BKK ACC Sector 3 airspace. A Korean registered Boeing 747, KAL362, had departed Kuala Lumpur for Seoul, tracking via B219 at FL270. Approaching KANTO, located to the west of KATKI, the aircraft was transferred to the BKK ACC. The crew of KAL362 contacted Bangkok Sector 3 and reported passing KANTO at FL270, estimating KATKI at 0219, and requesting climb to FL290. The next reporting position was SINMA, to the east of KATKI. At 0217:20 Bangkok Sector 3 cleared KAL362 to climb to FL290. KAL362 reported leaving FL270 for FL290. At 0220:21 the pilot in command of QF16 advised the Sector 3 controller of having received a traffic alert and collision avoidance system (TCAS) traffic advisory (TA), and that the aircraft had climbed to FL300 to avoid a collision with KAL362, but was now descending to FL290.					
Human–system interaction failure					
KAL362 was incorrectly given a clearance to climb to FL290 by the Bangkok Sector 3 controller, and that the crews of both QF16 and KAL362 were acting in accordance with the clearances issued to them. The procedural controller was responsible for issuing clearances to aircraft under procedural control, as was the case in this event. The role of the radar controller was to pass on the clearance to the aircraft. By not consulting with the procedural controller, the radar controller bypassed the established system of control, leading to a breakdown in safety. The KANTO flight progress strip for KAL362 should have been retained on the procedural board until the crew reported at SINMA, the next position. The removal of the KANTO strip by the radar controller removed the only reminder available to all controllers that the intended tracks of KAL362 and QFI6 would cross. Inclusion of the KATKI position on all flight progress strips for aircraft using the intersecting routes would have enabled controllers to more readily assess separation requirements in the procedural airspace. If the strips had required the KATKI position it is probable that the details for QFI6 and KAL362 would have been displayed under the same designator on the board, allowing controllers to recognise the potential conflict.					
Perspective of the designer					
• A controller with normal ability can deal with the problem. • The controllers will cooperate each other in order to check flight progress.					
Perspective of the operator					
• It is difficult to evaluate the progress of all flights without a memory assistance device such as a progress strip bay. • Monitoring frequency that requires continuous concentration of operators can easily fail. • In order to save space and as a short cut of procedure, a practice of removing strips that may be obsolete information is practical and does not harm the system.					
Design-induced error					
The design of the Sector 3 console did not allow for all relevant flight progress strips to					

be displayed. The configuration of the Sector 3 console provided insufficient space to adequately display all relevant flight progress strips. As a result, controllers had developed the habit of removing strips at the earliest opportunity, thereby creating the potential for vital information to be missed. The inability to monitor the control frequency while conducting coordination reduced the likelihood of the procedural controller maintaining a complete appreciation of the disposition of traffic. Design of the console may not provide supportive space for controllers' memory. Design of console and procedure may not provide an effective protective measure against information loss. Design of console may not consider monitoring difficulty of operators.
Related theories
Gulf of evaluation, Irony of automation- monitoring failure

Case number	5				
Date of occurrence	04/11/01	Source	ATSB	**Occurrence number**	200105351
Accident description					
The crew of a Boeing 767 (B767) had been cleared to taxi for departure from runway 01, intersection A7, at Brisbane. They proceeded along taxiway B then, incorrectly, initiated a turn onto taxiways B5 and A, which was in conflict with rapid exit taxiway A5S. A BAe146 vacating runway 01 via A5S, was instructed by ATC to hold short of taxiway A in order to avoid the B767. The crew of the BAe146, although not expecting to have to hold short of that taxiway intersection, had reduced speed to an extent that they were able to comply with the instruction.					
Human–system interaction failure					
The operator of the B767 advised that they had tried a new system of printing aerodrome charts from a computer application compact disk. However, the print format was such that the pilot in command of the B767 was not able to correctly read the notes provided on the chart with respect to taxiway routes and directions.					
Perspective of the designer					
● The new system of computer application will increase efficiency of control and automation.					
Perspective of the operator					
● The computer applicable system should provide information in relevant forms.					
Design-induced error					
• The new system that could not be printed in large format made it difficult for the pilot to distinguish characters between points in the chart.					
Related theories					
Gulf of evaluation					

8.3.1.2 Study 2: cases of purely human error

The primary accident analysis on the research dataset showed that 47% of all accidents in analysed documents were caused by "operator error" that was assumed to contain a concept of human–system interaction failures (Table 8.11).

Table 8.11 Different causations of accidents (ATSB, 1997 – February 2005)

Type	Number of cases*	Percentage
Mechanical failure	204	33%
Operator failure	287	47%
External factor	56	11%
Unknown	71	9%
Total	618	100%

* Double counting is allowed

With the documents that contain human error, the kinds of phenomena and how many times a concept of design-induced error appeared in the each case were examined. This answered the question: *What kinds of theory can be applied into a human–system interaction failure if you assumed that the failure contains phenomena of a concept of design-induced error?* This question and the resulting answers are useful to identify design issues in accident documents.

Theory explains the concept of design-induced error but it is not easy to describe all of such phenomena because they are psychological phenomena that need intensive investigation from a psychological point of view. It may be suggested therefore a proposition in this research that if a document describes a symptom of human error, then it may have been assumed that the case has a concept of design-induced error to some degree. Table 5.4 lists the categories of theory used (previously identified in chapter 4), and the numbers of report documents showing evidence of these theories.

Discussion: A meta-theory may help to recognise design issues in human–system interaction failure cases by applying the theory into the cases when we cannot exactly identify the issue due to lack of information in accident reports. Limitation of the meta-theory could be overcome by developing an investigation technique on human–system interaction failures.

8.3.2 Reasoning supporting with the developed ontology

It is necessary for a designer to understand in a design process how his/her design will be working with the operator because there are many unanticipated consequences of systems. In order to understand why an artefact has failed, the designer has to look through data or documents that have recorded previous experiences. This reasoning process is a kind of design rationale process because the reasoning is to find a reason behind decisions. Many reasoning support methodologies such as IBIS (Issue Based Information System)[Conklin, 1996] and PHI (Procedural Hierarchy of Issues) [McCall, 1991] have been developed [Lee, 1997].

One of the issues in the design reasoning support system is to enrich issues or questions for reasoning on searching for alternatives. Operators (i.e. users) in many cases live in another world from designers, which makes it difficult for designers to discourse with them. Capturing knowledge from users of a system is limited, not to mention failures. As a result, much knowledge comes from previous reports of failures. The concept of design-induced error can be treated as one of the design issues. The ontology developed may help designers to understand unreasonable consequences of design in a system. This thesis suggests two reasoning processes that can be used with the developed ontology.

8.3.2.1 consequences – cause – reasoning process

First, a "*consequences – cause – reasoning process*" can be applied for a design-induced error reasoning process. This process starts with searching for a *consequence* with concepts (i.e. "occurrence number", "occurrence data", or "accident") when a reader wants to see an unreasonable human–system interaction failure resulting from design.

The reader then moves to a *cause* phase. In this stage the reader checks what kind of error the operator made, and what was the uncompleted task in the error. In the *reasoning* phase, there are two steps. First, he/she can find what kind of design failed in human–system interaction by searching for "system" and "error-inducing design" concepts.

Finally, the reader can understand why the design failed and the operator's perspective in the occurrence by matching the design-induced error theory with human error.

An example of this approach is shown in the following case.

Consequences – Cause - Reasoning case:

[*Consequence*]

Occurrence number: "199403314"

Occurrence date: "09 November 1994"

Incident: "failure of the left engine due to fuel starvation"

[*Cause*]

Human error: "mismanagement of the fuel system"

Problem area: "the time taken for the outboard fuel tanks to empty, the orientation of the cockpit fuel selector switches"

[*Reasoning1*: design issues with human error]

System: "fuel system"

Error-inducing design: "there were two significant differences between the fuel system in aircraft SPP and that of other Aero Commnader models the pilot had flown"

[*Reasoning2*: theory and recommendation for designers]

Theory: design affordance theory explains how such failure can happen when a design of a system is different from the design of a similar system that was familiar to operators.

Recommendation: When designing a modification of a system from previous systems, it should be considered what the differences are from previous or other system in format (e.g. position, operation, or procedure) of the system and then test whether such changes have a possibility to confuse operators in a critical condition.

This case is shown in a diagrammatic form, based on developed in Chapter 7, in Figure 8.7.

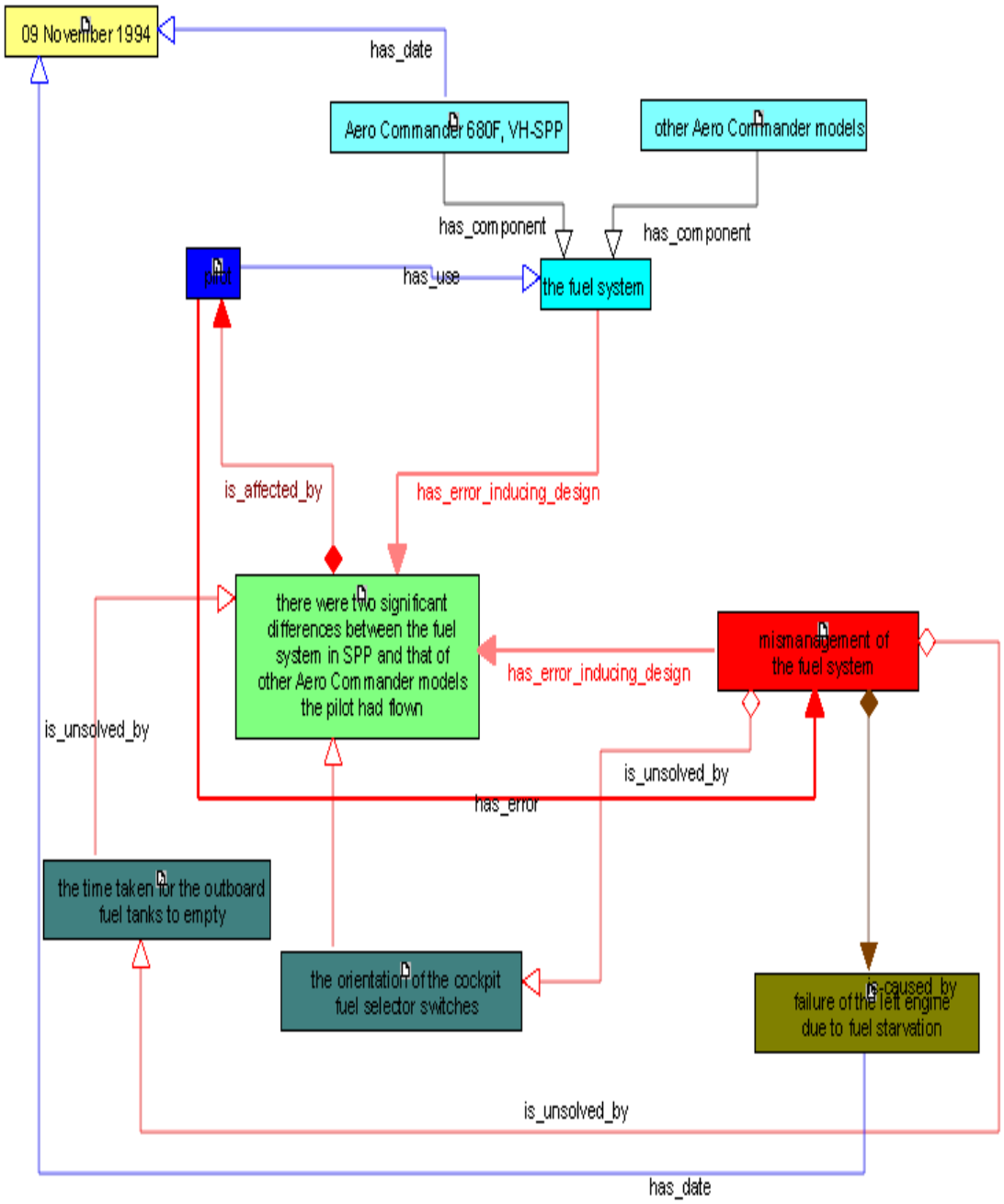


Figure 8.7 An example of ontology of accident cases

8.3.2.2 issue – idea – argument process

Secondly, the "*issue – idea – argument process*" can be used for a design-induced error reasoning process. In this process *issue* refers to human error, *idea* refers to error-inducing design, and *argument* refers to design-induced error theory (Figure 8.8).

It begins with a question that raises a human–system interaction failure by questioning "why the operator mismanaged the artefact at the time of the accident?" in the above case. An idea then prompts, "the feature of the artefact was different from other models of similar type of the system" by looking at a concept of error-inducing design.

The design-induced error theory including the ontology can help to raise an argument of design issues with human error: "a different feature in a same type of artefact can make human operators easily confused with the feature because they have in mind that similar systems have similar features in operation."

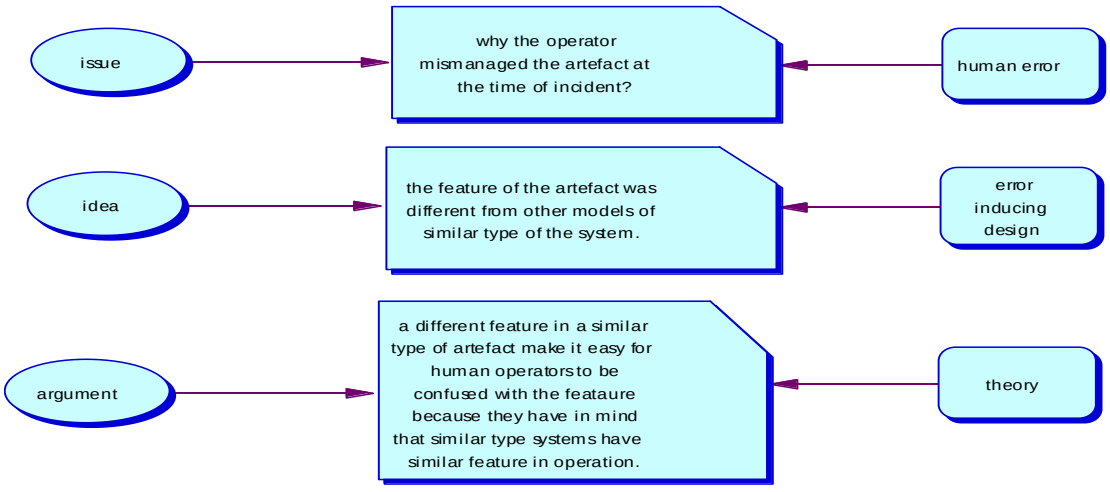


Figure 8.8 The issue–idea–argument method for reasoning on the concept of design-induced error

8.4 Investigation on knowledge representation

One of important roles of ontology is to analyse domain knowledge [Noy and McGuinnes, 2003]. The hierarchy of ontology represents entities and relations in a concept that might be mapped ontologically when attempting to provide a full set of conceptual areas, in which we can identify the areas of interest for supporting discourse during design-induced error capture. In order to represent the concept well, it is necessary to define clearly the related concepts and their relationships. The ontology developed has three main parts in the relation map: design, human error, and theory (Figure 8.9).

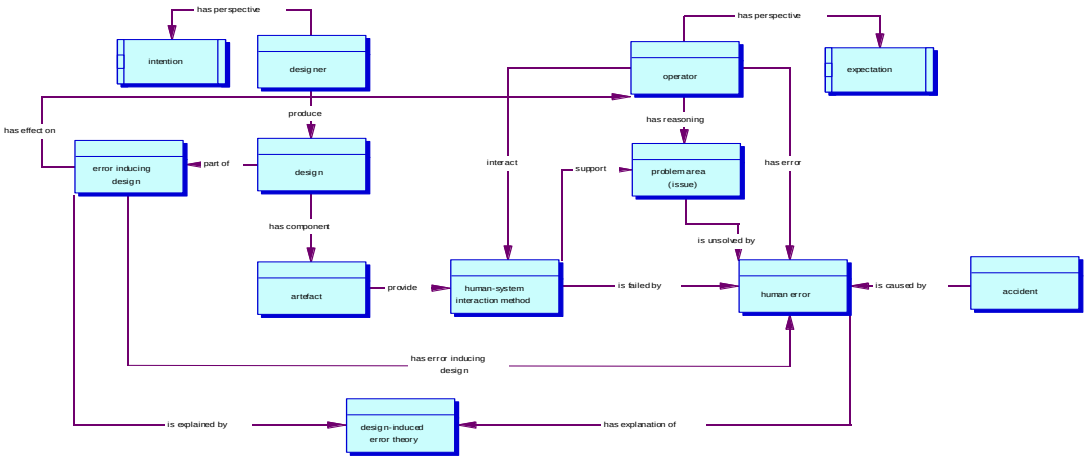


Figure 8.9 The ontology of design-induced error with the concepts and relations

The developed web browser in PCPACK shows the relation between related concepts (Figure 8.10). From this browser users can work through design and human error by clicking a related term in a page. This makes it easy to search for a relation between design and human error.

For example, if a designer selects an artefact or system (left side in the PCPACK browser) he or she can see related cases of human errors or phenomena (right side in the PCPACK browser).

Discussion: If the cases of design-induced error can be accumulated it will be more useful to present relationships between design and human error.

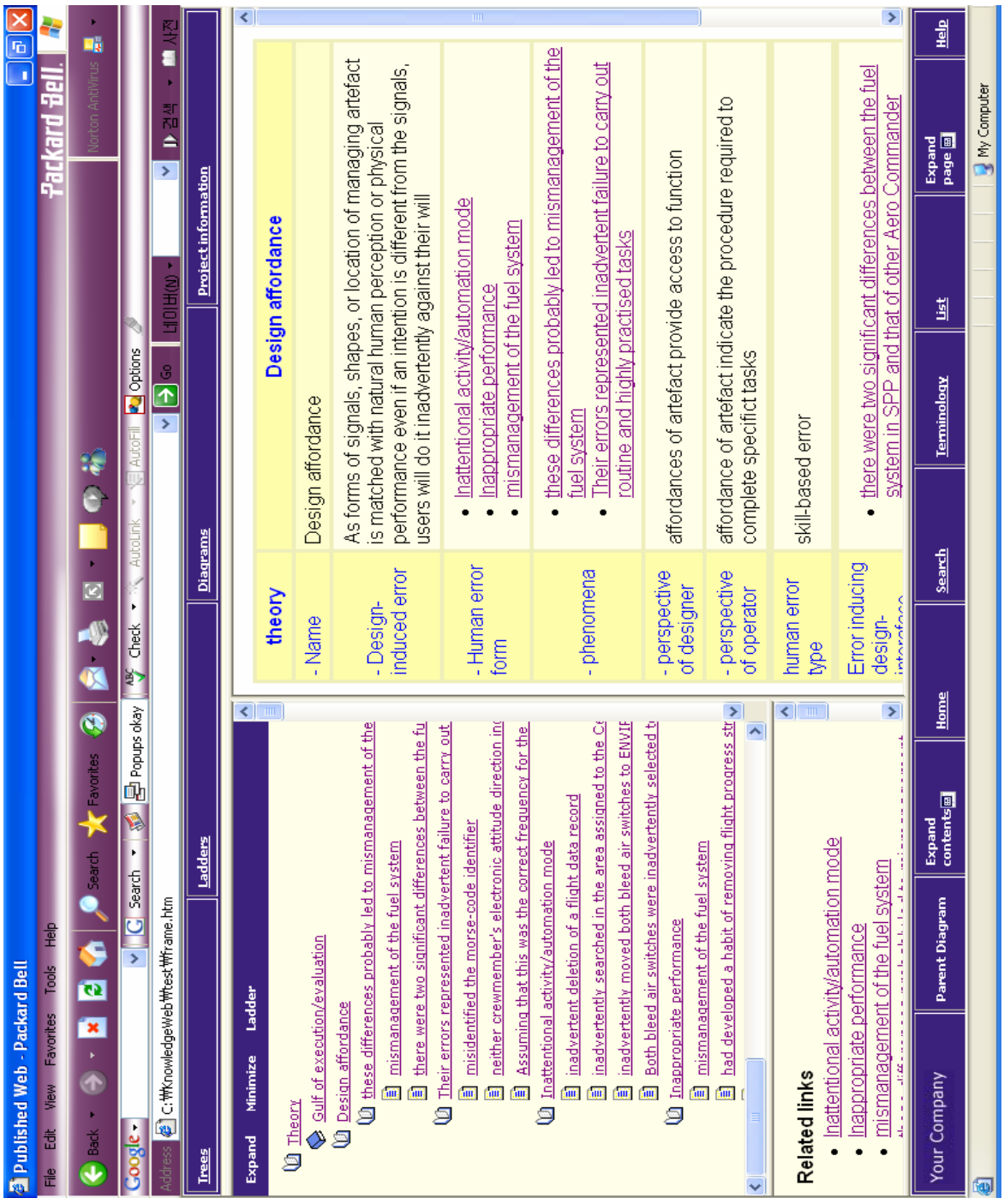


Figure 8.10 The published ontology browser by the PC PACK publishing tool

8.5 Investigation on a knowledge acquisition issue

Manual description analysis of the accident reports revealed that a domain analysis for searching for a specific issue (for example, in this research, finding design issues in accident reports) is a time consuming task. The analysis of accident reports in terms of design-induced error took several months.

The developed ontology in PCPACK can aid people to acquire knowledge in which they are interested with an annotation (mark-up) tool. The Protocol tool saves files in a form of XML formation with marked text.

The ontology provides items of concepts, attributes, relations related to the ontology. Readers can mark up domain documents according to the predefined concept categories. While reading a document a reader can annotate words or sentences by using highlight (mark-up) pens in the Protocol tool if he/she finds that the description is matched with defined concepts. The annotated reports are saved in a form of XML file (see Figure 8.11).

After that the PCPACK Diagram tool helps to connect between annotated texts by using defined relations in the ontology. The reader can link concepts by clicking nodes. If this work has been done, the ontology browser automatically captures and represents the relationships between marked concepts in web pages. The reader can also review relations between concepts in tree or diagram forms.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <Protocol Origin="file://RPC-ENPIJS/C/Documents and Settings/shin/My
  Documents/accident analysis/accident reports txt file/200001827.txt">
- <Markups>
- <Markup ID="648" Position="19" ContextOffset="19">
  <Parent ID="33" NAME="Occurrence_Number" />
  <Text>200001827</Text>
  <Context>Occurrence Number: 200003056</Context>
  </Markup>
…..
- <Markup ID="706" Position="9121" ContextOffset="0">
  <Parent ID="132" NAME="Not_Providing_Information_or_Functions" />
   <Text>The manufacturer's Pilot's Operating Handbook did not specify checks for
    crossfeed operation or positioning the fuel selectors to the off position to observe a
    decrease in fuel flow</Text>
   <Context>http://www.atsb.gov.au/publications/investigation_reports/2000/AAIR/aair200
    003056.aspx</Context>
  </Markup>
……..

  </Markups>
  <PostIts />
  </Protocol>
```

Figure 8.11 An example of annotated XML files

8.6 Summary

Table 8.12 presents the summary of investigation on knowledge sharing issues examined in this chapter.

The investigation of the developed ontology revealed what is possible and what is not, of the research aims and objectives.

(1) It may not possible to distinguish design-induced error from other types of human error because the error forms are the same.

(2) It is necessary to design evidence levels for a specific domain in order to find a design-induced error in accident reports because the evidence of a concept of design-induced error depends on description of documents.

(3) It may not possible to extract a case of design-induced error automatically because of the diversity of expression of design issues related to human error and the evidence issue in (1) above.

(4) An annotation scheme (mark-up) in accident reports will improve to formulate a concept of design-induced error.

(5) The meta-theory of design-induced error is useful to recognise different perspectives between designers and operators in a case of human–system interaction failure.

(6) The ontology developed may be helpful for designers to recoginse relationships between design and human error.

(7) The ontology browser can help people to reason about design issues in human–system interaction failures.

Table 8.12 The summary of investigation on knowledge sharing issues

INVESTIGATION ISSUES	METHODS APPLIED	OUTCOMES	REFERENCE
Evidence issue – How to provide evidence of design-induced error in accident reports?	– Manual description analysis on ATSB reports	– 5 scales for 287 cases	Chapter 5
Knowledge retrieval issues – What are the keywords of design-induced error?	– Manual description analysis	– Identify keywords and clarify 4 description category of them (defective cognition, performance problem, knowledge problem, distracted cognition, reliance on systems)	Chapter 7
Is there any possibility to extract related concepts in effective or automatically?	– Keyword search method for the human error and design issue (Google search engine), – Annotation scheme with Ontology	– One case study Two terms examined in ATSB – 52 annotations in developed ontology	
Knowledge reasoning issues – How does the developed ontology help people to think about design issues in human error?	– Evaluation of captured cases with the theoretical model (V^2 analysis) and knowledge based information tools (PCPACK, Protégé, Google) – Consequences-cause-reasoning process, issue-idea-argument process	– Tested with examples (with Chapter 5 case study) – Web browser in PCPACK one example presented	Chapter 5 Chapter 7
Knowledge representation issues Is it effective way of knowledge representation (KR) of the concept of design-induced error?	– PCPACk template – PCPACK browser – Protégé hierarch	– Knowledge model diagram in PCPACK – Users can find the relations in the PCPACK web browser or Protégé	Chapter 7

Chapter 9. Conclusions

The research described in this thesis considered design as one of the important factors influencing human error. This thesis was tried to answer the questions: how design affects human operators; how such adverse influences can be analysed; and the benefits of analytical tools developed in this thesis.

This thesis has presented a proposed model of human error influenced by design in the meta-theory of design-induced error. An ontology that categorises human error and related design issues has been developed using a knowledge-based software methodology. The developed model (a meta-theory of design-induced error) and the ontology (a knowledge model) particularly were tested using report documents of real accident cases.

The literature review indicated that previous research in this field has attempted to explain phenomena that arose during operations in the field, such as cases of automation surprise [Sarter et al., 1997] in the domain of aviation. The cases studied show that even if there were no apparent engineering failures in the accidents, rather they seemed to be just caused by a human operator, it is possible , however, to pick out hidden issues as fundamental causations of human errors. The theories that have explained phenomena related to human–system interaction failures are, at least partially, affected by the design of the system. It is also discovered that designers' understanding of operators' performance is principally limited to their own expectation and experiences.

Many of these theories, however, stand alone, with little attention being given to their relationships with each other. No one has tried to integrate these theories with regards to local rationalities between designers and operators that could affect human–system interaction failures. Each theory would indicate design issues in human–system interaction failures in a particular condition but not all conditions. It does not explain whole design issues in human–system interaction failures. Therefore, the designer would find it difficult to capture all the relevant knowledge contained in theories.

Three research issues have been raised to help people who want to develop safer systems:

- What is the nature of the hidden influences of a design in modern complicated and automated systems?

- In what ways could a designer be assisted to recognise design issues in human error?
- While several theories explain the issues respectively, is there any effective way to deliver a collective view of related theories to people who need to recognise the issues?

This research attempted to introduce a meta-theory in order to provide a collective view on the theories with a concept of design-induced error. The concept of design-induced error, in this thesis, refers to inappropriate roles of design in human–system interaction. A "meta-theory" makes it possible to provide a collective view of the theories by adopting meta-theoretical paradigms and assumptions taken from investigation of underlying structures of theories. The paradigm in this meta-theory of design-induced error is a contextual paradigm of different perspectives between designers and operators that are considered as playing a key role in the phenomena. We can interpret each theory in terms of local rationalities. In order to combine related theories, an ontological assumption was used with three layers of human–system interaction perspectives; affordance level, psychological logic level, and trust level. The three perspective layers could explain all levels of phenomena that express design issues in human–system interaction failures.

In order to make up a meta-theory of design-induced error, seven theories that present design issues in human–system interaction failures were identified and applied to design-induced error in this thesis: gulf of execution/evaluation; design affordance; irony of automation; trust in automation; glass cockpit problem and automation surprise; risk homeostasis; and plan delegation. In the model the phenomena of design-induced error are interpreted by local rationalities between designers and operators.

For a practical point of view of this thesis, knowledge management technologies were used. A web-based knowledge management system and technologies are a promising area to share knowledge between experts (e.g. psychologists in human error) and users (e.g. designers). In order to deliver the issue above effectively, this research had extended into developing an ontology of design-induced error based on the meta-theory, in which the ontology helps people to recognise design issues in human error cases. This process included the work of classifying entities and identifying relationships between the entities in a concept of design-induced error.

Accident reports provide an important resource for the designer to understand human activity, the mechanisms underlying error, and the development of effective countermeasures to prevent the recurrence of these errors [Petroski, 1994; Bruseberg et al., 2003]. Nowadays, many of these reports appear on World-wide Web in HTML (or

XML) Form. The trend will grow so rapidly in future that the development of knowledge capturing and reasoning methodology in the system will be a more important issue than before for designers as well as accident analysts.

As a prototype experiment of knowledge acquisition and knowledge modelling for design-induced-error reasoning, Australian aviation accident and incident reports were tested and evaluated. The NTSB (National Transportation Safety Board, USA) and ASN (Aviation Safety Network) accident database systems also were used for information retrieval experiments in design-induced error reasoning. The developed web-based ontology browser of design-induced error with relevant accident cases is presented as a CD with this volume. Additionally, the limitations of this model and the research methods employed are also discussed.

9.1 Concluding arguments

It is said that designers have a different view of a system from operators [Norman, 1998; Woods, 2000 etc.]. Many human-error researchers have shown how some kinds of design have failed to prevent human error and indeed have exaggerated and contributed to such errors.

Human-error experts have argued that design, especially in modern complex and automated systems, inherently affects an operator's cognition and performance, resulting in human error (termed "design-induced error" in this thesis). They have described phenomena of design leading to human error in various theories.

Designers, however, have difficulty understanding the knowledge that human error experts have suggested because: (1) Theories that explain design issues in human error are not unified and they are scattered in different theories; and (2) Meanings in theories need to be interpreted by psychological theories with phenomena and symptoms, not the engineering logics that are familiar to engineers.

It has been argued in this thesis that in order to encourage designers to have correct reasoning on human–system interaction, it is important to share the knowledge that human-error experts have. And one of issues of improving knowledge sharing on human error is to provide designers with "an effective reasoning support tool" that can help them to search for and infer issues related to design and human error.

In order to achieve the goal of enabling designers to have the same view on human error as human error experts, this research aimed:

(1) To provide "*an interpretational tool*" (i.e. a theoretical methodology) that can help people to search for design issues in cases of human–system interaction failures by

developing an integrated model synthesising related theories;

(2) To develop "*a knowledge-based reasoning support tool*" that can be used for understanding relationships between design and human error in accident cases by visualising the relationships.

Accident reports are used as a repository basis in this research for developing and applying a knowledge-based ontology model of design-induced error because they have lot of information including the concept of design-induced error. They are good sources for gathering lesson-learned knowledge. From these failures, we have an opportunity to know how operators think about systems. However, it is still difficult to search for and understand the concepts in the documents without effective methodologies.

1. Development of an interpretational tool (meta-theory of design-induced error)

When you look at an accident report that contains human error, without any knowledge of human error, it is difficult to find design issues without a relevant interpretational tool. Rather you may assume or get the impression that the error in the accident case originated from wrong human thinking or performance, not from design-related issues. However, equipped with a reasonable human-error interpretational tool, you can raise the question of design issues influencing human error from the same case.

An integrated model synthesised related theories that explain design issues in human–system interaction failures.

The tool developed in this research will help people to have reasoning on design issues from human error. For example, if you found a case where the automatic reaction of an operator was involved in causing an accident, you can refer to a concept of "design affordance", which explains that if two functional designs of a system are similar in form, it will induce a user to make an error in certain circumstances. You can understand what kinds of design issues can appear in a human–system failure by applying meta-theory in the tool into an accident case.

2. Development of a knowledge-based reasoning tool (a knowledge representation model for design-induced error)

This research was based on two methodological practices: (1) web-based knowledge

acquisition and representation methodology, (2) use of ontology.

Web-based knowledge acquisition and representation techniques are useful in current and future design environments. This research has provided a web-browser style visual knowledge representation tool that can help to search for and understand the concept of design-induced error.

Ontology has been used for codification of domain knowledge. It will be useful if we can develop a formal description of design-induced error. However, the project did not intend to develop an extremely formal and detailed ontology of design-induced error, but a conceptual and prototype ontology (with a small and particular domain, i.e. Australian aviation accident reports).

The developed tool aims to support designers to reason on design issues as follows:

To provide possible relation categories in a web browser, in which people can search related concepts and instances systematically by clicking a concept in which they are interested because the browser shows related concepts, which are stored in the ontology, in a page;

To provide diagrams of accident cases, in which people can capture a relationship between design and human error because the diagram shows concepts graphically, with lines connecting each concept.

9.2 Achievements

The aims of this thesis presented here are to examine the influence of design on human error, and to find effective methods to share knowledge taken from human error theories that describe human–system interaction failures (i.e. human error) in terms of the role of design. For its aims the thesis proposed a meta-theory of design-induced error, an integrated and collective view on these theories, in order to present better understanding of how design induces human errors. This thesis then developed an ontology of design-induced error based on the meta-theory in order to make it possible to capture the issues from accident reports. They are main objectives of the research.

The main aim of this research was; to develop a meta-theory of design-induced error suitable for use in human–system failure analysis that enables the designer to understand such phenomena in terms of the role of design. For the aim, five objectives presented in Chapter 1 have been fulfilled through the research.

9.2.1 Objective 1

To identify the issues involved in influence of design on human errors

Chapter 2 reviewed the literature on human-error theories in order to identify related human error theories and issues involved in the influence of design on human errors. The chapter reviewed a general human-error model developed by Rasmussen and Reason that is recognised by most human-error theorists. Seven theories were identified as showing relationships between design and human error: gulf of execution/evaluation, design affordance, trust in automation, glass cockpit problem, automation surprise, risk homeostasis, plan delegation. Each theory was examined with accident cases. The theories theorised the manner in which the performance and cognition of humans are influenced by design while interacting with an artefact or systems. The influences are sometimes not apparent because they have slowly degraded the abilities of human operators. The characteristics of modern design adopting computerised and automated functions and systems were also examined. The review identified that temporal decision-making conditions are identified the main characteristics and issues of the influences of current design.

9.2.2 Objective 2

To develop a collective model taken from related theories that describe relations between design and human error

The underlying characteristics of related theories were investigated in chapter 4. The chapter also examined the design concept assumed in related theories. The local rationality theory was adopted as a paradigm to binding these theories. By the adopted paradigm, the theories can be shown in a collective model.

The next step was to categorise design types and human–system interaction patterns into four design types and three interaction patterns. The four design types are; feature, function, logic, and reliability design, and they have relations with the three human–system interaction levels; affordance, psychological logic, and trust level of interactions. It is assumed in the model that a failure of human–system interaction occurs when each design does not match with related levels of interactions.

9.2.3 Objective 3

To analyse accident cases with the framework developed

Chapter 5 examined the collective model by applying it to accident cases. The Australian aviation accident report system (AAARS) was chosen to provide data for the experiment.

9.2.4 Objective 4

To develop a knowledge model of capturing useful texts in the description of accident documents

The fourth objective was addressed through a literature review of knowledge-management methodology, and the application of a knowledge-management software to the development of a knowledge model of design-induced error (chapter 7).

9.2.5 Objective 5

To demonstrate how developed models can help to analyse

accident cases that include design issues in human errors

The last objective was achieved through investigating accidents in chapters 5 and 8.

The following are the achievements of the research:

(1) A concept of design-induced error has been developed in order to understand human–system interaction failures effectively introduced in Chapter 1.

(2) An interpretational method (model) of human–system interaction failures has been developed (i.e. a meta-theory of design-induced error) developed in Chapter 4.

(3) Current theories relevant to design issues and human error have been integrated into the model developed in Chapter 4.

(4) The concept of design-induced error has been formalised in terms of local rationalities between designers and operators in Chapter 4.

(5) A theory-based ontology of design-induced error has been created in Chapter 7.

(6)Visualisation of the concept of design-induced error and its relationships with other concepts has been provided by developing an ontology-browser of design-induced error developed in Chapter 7.

(7) This has been tested in accident reports and used to interpret the accident cases in terms of the concept of design-induced error in Chapter 5.

(8) The understanding of design issues in relation to human–system interaction failures has been improved by providing a knowledge acquisition and representation methodology to take the place of the manual description analysis of accident reports when searching for design issues in human–system failure report documents discussed in Chapter 8.

(9) A mark-up method (annotation technique) for the knowledge acquisition of a concept of design-induced error in accident report systems has been provided developed in Chapter 7.

9.3 Recommendations and further works

Human-error research has contributed to the development of safety design. Various models help people to understand related issues. Although these models have been developed, there has been no synthesised model to illuminate the role of design on human errors.

The model of the meta-theory of design-induced error (in chapter 4) may provide valuable insights into ways to recognise adverse results of design in the early stage of design process.

The findings from the evaluation of accident reports in terms of design-induced error in chapter 5 and the ontology developed in chapter 7 may be useful to capture design issues in accident documents. It would be hopeful that these findings fill gaps between designers and users in understanding of the consequences of a design innovation or modification.

9.3.1 Recommendation for those interested in human–system interaction failures

For designers and systems developers who produce artefacts and systems:

(1) It is necessary to understand operators' expectations as to designers' intentions in the design of an artefact or a system.

(2) The designer should consider the possibility of unexpected use of artefacts or systems when developing or modifying them.

(3) In order to understand how design affects the performance and cognition of operators, the functions, procedures and appearance of an artefact or a system should be checked and tested in design processes in terms of the concept of design-induced error.

For authorities who investigate accidents and produce accident reports:

(1)It is necessary to develop techniques to rectify design issues in operator failures. This research identified that some accident reports do not have enough discussion about the role of design issues in human–system interaction failures.

(2) It is necessary to develop systematic methods for investigation and description of design issues that affect operators' cognition and performance.

(3) More concern should be taken over design-induced error by comparing design intention and operator expectation with design expectation and operator intention.

① They should develop mark-up tools for users to interpret the accident reports for their own purposes.

For readers/researchers who interpret accident reports in order to identify design-induced error:

(1) To understand the role of design is important to analyse human–system interaction failures.

(2) To use the interpretational tool (the meta-theory of design-induced error) to identify design issues in human errors.

9.3.2 Limitation of the research

For the research, there were areas of limitation of the research methodology, research area, and developed model or ontology.

Limitation of research methodology;

(1) This research is not a pure ontology study or psychological human-error study, but a hybrid between cognitive theories and engineering and information technology.

(2) This research is limited to study of Design-induced error, not research on all forms of human error.

(3) This research is not research on how to construct an entire knowledge-based system (KBS), rather to develop an ontology of Design-induced error that may be used in a KBS.

(4) The research has tried to use current Web-based reporting systems, but it does not involve changing accident report systems or content of the reports.

Limitation of the development of meta-theory of design-induced error:

(1) The aim of the research is to try to find a way synthesising existing theories of how design induces human error, not to replace them.

(2) There is not one, unique meta-theory.

(3) The function of the meta-theory is to help generate an ontology of the properties of design-induced error.

(4) The purpose of the ontology of design-induced error is to help designers interpret reports of particular accidents and incidents.

Limitation of the developed knowledge-based ontology of design-induced error:

(1) It was not a detailed and complete constitution of ontology research but a prototype study for the subject of the research, i.e. in order to examine and demonstrate effective ways to capture and represent implicit psychological knowledge.

(2) The area of developed ontology presented in this thesis was specified and limited to the Australian aviation accident incident reporting system. As a result, it is necessary to extend and modify the ontology to apply the ontology in another domain.

9.3.3 Further work

It has been my experience that the proposed idea was useful for interpreting human–system interaction failures, and the ontology that had been developed in order to extract and represent relevant knowledge and their relationships would be advantageous to understand the psychological concepts. Work could be undertaken in order to develop more useful models to interpret human–system interaction failures from the model suggested in this thesis. The ontology developed in this thesis for a prototype can be developed further in practical areas such as aviation. Several areas of the documented research could be investigated further. These included:

Firstly, the most important area requiring further investigation is how to enrich and make more concrete the meta-theory of design-induced error. This would involve investigation of other theories that explain design issues in human errors. Further investigation to clearly define the relationship between design purpose, design concept, and human–system interaction type would help the task.

Secondly, guidelines for identifying design issues in human–system interaction failures in accident investigation need to be formulated. The guidelines would be helpful for accident investigation authorities and engineering designers to refer to. They should also be formulated to provide useful information about design questions to designers.

Thirdly, the ontology developed in this thesis needs to be further tested, modified, and extended into applied areas. It would be of great interest and applicability to further develop this work for other domains. This could then ensure that the ontology of design-induced error can be applicable in other domains. The more instances populated, the more useful the ontology.

Fourthly, the ontology developed in this research can be used for tackling this type of problem with the natural language processing (NLP) methodology and machine learning process. This can be used for developing a fully machine-understandable form of accident reports. Limitations of understanding human-generated documents could be overcome with knowledge technologies.

Finally, the research can be used for developing a simulation technique of human–system interaction failures, which show people a visual demonstration of a failure, from accident reports. Those efforts may increase the usability of accident documents for different approaches of accident analysis without damaging the original contents of the document.

References

Abar, S., Abe, T., Kinoshita, T. 2004. "A next generation knowledge management system architecture, Advanced Information Networking and Applications", AINA 2004. 18th International Conference, Vol. 2, Issue , 29-31, March 2004, Page(s): 191–195.

Abdalla, R. M., and Teufel, S., 2006. "A Bootstrapping Approach to Unsupervised Detection of Cue Phrase Variants", Proceedings of the ACL 2006.

Abdullah, M.S., Benest, I., Evans, A., Kimble, C. 2002. "Knowledge modelling techniques for developing knowledge management systems", 3rd European Conference on Knowledge Management, Dublin, Ireland, September 2002. ISBN: 0-9540488-6-5, pp 15-25

Adams, J. 1995. *Risk*. Guildford and King's Lynn, England: Biddles Ltd.

Alkov, R.A. 1997. "Human error" in *Aviation safety. The human factor*. Casper, WY: Endeavor Books, 75-87.

Bainbridge, L. 1983. "The ironies of automation". *Automatica*, 19, 775-780.

Bardram, J. 1998. "Designing for the dynamics of cooperative work activities", Proceedings of CSCW 98, 89-98. New York, NY: ACM.

Barthelmess, P., Anderson, K.M. 2002. "A View of Software Development Environments based on Activity Theory", *Computer Supported Cooperative Work Archive*, 11:1-2, 13-37.

Bartolone, A., Trujillo, A. 2002. "Glass-cockpit pilot subjective ratings of predictive information, collocation, and mission status graphics: an analysis and summary of the future focus of flight deck research survey", National Aeronautics and Space Administration, Langley Research Center, Hampton, Virginia, NASA/TM-2002-211419, January 2002.

Bhaskar, R. 1978. *A Realist Theory of Science*. New York: The Harvester Press.

Billings, C.E. 1997. *Aviation automation: The search for a human-centered approach*. Mahwah, NJ: LEA.

Blessing, L.T.M., Chakrabarti, A., Wallace, K.M.. 1995. A design research methodology, Proceedings of the International Conference on Engineering Design, ICED 95, Prague,

22-24 August 1995, WDK, Heurista Zürich pp 50-55

Borycki, E., Kushniruk, A. 2005. "Identifying and preventing technology-induced error using simulations: Application of usability engineering techniques", *Health Care Quarterly*, 8, Special issue, October 2005.

Bouthillier, F., Shearer, K. 2002. "Understanding knowledge management and information management: the need for an empirical perspective", *Information Research*, Vol. 8 No. 1, October 2002 (available at: http://informationr.net/ir/8-1/paper141.html, accessed 18 February 2005).

Bruseberg, A., Johnson, P. 2003. "Understanding human error in context: approaches to support interaction design using air accident reports." In: Jensen R (ed.): *Proceedings of the 12th International Symposium on Aviation Psychology*, 14-17 April 2003, Dayton, Ohio, USA, 166-171.

Busby, J.S., Hibberd, R.E. 2002. "Mutual misconceptions between designers and operators of hazardous systems", *Research in Engineering Design*, 13, 132-138.

Busby, J.S., Hibberd, R.E. 2004. "Artefacts, sensemaking and catastrophic failure in railway systems", Systems, Man and Cybernetics, 2004 IEEE International Conference, 10-13 Oct. 2004, Volume: 7, pp. 6198- 6205

Busby, J.S., Hughes, E.J. 2003. "How plan delegation contributes to systemic failure", *Human Systems Management* 22, 13-22.

Busby, J.S., Mileham A.R., Hibberd, R.E., and Mullineux G. 2004, 'Failure modes analysis of organisational artefacts that protect systems', *Proceedings of the Institute of Mechanical Engineers Part B*, vol 218(9), pp 1211-1215

Busby, J.S., Strutt, J.E. 2001. "The derivation of hazard criteria from historical knowledge", *Journal of Engineering Design*, 12:2, 117-129.

Chandrasekaran B., Josephson J.R. and Benjamins V.R. 1999. What are Ontologies, and Why Do We Need Them?, IEEE Intelligent Systems, Vol.14, No. 1, pp. 20-26

Chapanis, A. The Chapanis Chronicles: 50 years of Human Factors Research, Education, and Design, Aegean Publishing Company, Santa Barbara, CA, 1999.

Cocchiarella, Nino B. 2001. "Logic and ontology", *Axiomathes*, 12, 117-150,

CommonKADS Course Material, 2003. University of Amsterdam, The Netherlands (available in http://www.commonkads.uva.nl/INFO/course-slides).

Conklin, J., 1996. The IBIS Manual: A Short Course in IBIS Methodology.

Corbridge, C., Rugg, G., Major, N., Shadbolt, N., Burton, A.M. 1994. "Laddering: Technique and Tool Use in Knowledge Acquisition", *Journal of Knowledge Acquisition*, 6, 315-341.

Court, A.W. 1995. "Modelling and classification of information for engineering designers", PhD thesis, University of Bath.

Cully, S.J. 2004. "Design for X", unpublished paper presented at internal seminar of the Department of Engineering , University of Bath, May 2004.

Darlington, M. 2002. "Cognition and the engineering design requirement", PhD thesis, University of Bath.

Davenport, T.H., Prusak, L. 1998. *Working Knowledge: How Organisations Manage What They Know.* Boston, MA: Harvard Business School Press.

De Keyser, V. 1990. "Temporal decision making in complex environments", Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences, Vol. 327, No. 1241, Human Factors in Hazardous Situations (Apr. 12, 1990), pp. 569-576.

Denny, M. 2002. "Ontology Building: A Survey of Editing Tools, 6 November 2002" (http://www.xml.com/pub/a/2002/11/06/ontologies.html).

Denny, M. 2004. "Ontology Tools Survey, Revisited, 14 July 2004" (http://www.xml.com/pub/a/2004/07/14/onto.html).

Dörre, J., Gerstl, P., Seiffert, R. 1999. "Text mining: Finding nuggets in mountains of textual data", In Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (SIGKDD'1999), San Diego, CA. pp. 398–401.

Dutta, D., Wolowicz, J.P., 2005. "An Introduction to Product Lifecycle Management (PLM)". In *Proceedings of the 12th ISPE International Conference on Concurrent Engineering: Research and Applications*, Fort Worth, Texas, USA, July 25-29, 2005.

Federal Aviation Administration, 1996. Human Factors Team Report on: The Interfaces Between Flightcrews and Modern Flight Deck Systems, June 18, 1996.

Festinger, L. 1975. *A Theory of Cognitive Dissonance*. Stanford, CA: Stanford University Press.

Flach, J.M., Dominguez, C.O. 1995. "Use-centred design", *Ergonomics in Design*, 19-24.

Geller, E.S. 1995. "Do we compensate for safety?", Blacksburg, VA: Virginia Polytechnic Institute. 9pp..

Gennari, J., Musen, M., Fergerson, R., Grosso, W., Crubézy, M., Eriksson, H., Noy, N. and Tu, S. 2002. "The Evolution of Protégé: An Environment for Knowledge-Based Systems Development" (available in http://www-protege.stanford.edu).

Gibson, J. J., 1977. "The theory of affordances", In Shaw, R., Bransford, J., (Eds,). "Perceiving, acting, and knowing: Toward an ecological psychology", (pp. 67-82). Hillsdale, NJ: Lawrence Erlbaum.

Gorbachev, B.I. 2003. "The causes and scenario of the Chernobyl accident, and radioactive release on the CHNPP Unit-4 site". Journal Title;KURRI KR, Journal Code:L2982A, ISSN:1342-0852,Vol.79;pp.28-44(2002)

Gourlay, S. N. 2004. 'Tacit knowledge': the variety of meanings in empirical research. Fifth European Conference on Organizational Knowledge, Learning and Capabilities Innsbruck, Austria, 2-3 April

Gruber, T.R., 1995, " Toward principles for the design of ontologies used for knowledge sharing", International Journal of Human-Computer Studies, 43, 907 – 928

Gruber, T.R. 1993. "Toward principles for the design of ontologies used for knowledge sharing", in N. Guarino and R. Poli (Eds), *Formal ontology in conceptual analysis and knowledge representation*. Kluwer Academic Publishers, in press.

Gruninger, M., Fox, M. S., "The role of competency questions in enterprise engineering". In Proceedings of the IFIP WG5.7 Workshop on Benchmarking - Theory and Practice, Trondheim, Norway, 1994.

Guarino, N. 1998. "Formal ontology and information systems", *Proceedings of FOIS'98*, Trento, Italy, 6-8 June 1998. Amsterdam: IOS Press, 3-5.

Halverson, C.A. 2002. "Activity theory and distributed cognition: Or what does CSCW need to do with theories?", *Computer Supported Cooperative Work*, 11:1-2, 243-267.

Harris, D., Stanton, N.A., Marshall, A., Young, M.S., Demagalski, J., Salmon, P. 2005. "Using SHERPA to predict design-induced error on the flight deck", *Aerospace Science and Technology*, 9:6, 525-532.

Hearst, M., 1999. Untangling text data mining. In Procedings of the 37th Annual Meeting for Computational Linguistics (pp.3-10).

Heylighen, F. 2002. "Complexity and Information Overload in Society: why increasing efficiency leads to decreasing control", Belgium: Free University of Brussels

Hicks, B.J., Culley, S.J., Allen, R.D., Mullineux, G.A. 2002. "Framework for the

requirements of capturing, storing and reusing information and knowledge in engineering design", *International Journal of Information Management*, 22, 263-180.

Hoffman, R., Shadbolt, N.R., Burton, A.M., Klein, G. 1995. "Eliciting Knowledge from Experts: A Methodological Analysis". *Organisational Behavior and Decision Processes*, 62:2, 129-158.

Hollan, J., Hutchins, E. and Kirsh, D. 2000. "Distributed cognition: Toward a new foundation for human-computer interaction research". *ACM Transactions on Computer-Human Interaction*, 7, 174-196.

Hollnagel, E. 1992. "The reliability of man-machine interaction", *Reliability Engineering and System Safety*, 38, 81-89.

Hollnagel, E. 1998. *The Cognitive Reliability and Error Analysis Method*. Oxford, UK: Elsevier Science Ltd.

Hollnagel, E. 2001. "Extended cognition and the future of ergonomics". *Theoretical Issues in Ergonomics*, 2, 309-315.

Horne, R.Adm. R. 1990. Address to NATO AC/243 Panel-8/RSG.14. Washington DC: US Naval Sea Systems Command.

Horvath, I. 2001. "A Contemporary Survey of Scientific Research into Engineering Design", In S. Culley & et Al. (Eds.), Design research - theories, methodologies, and product modelling, 13th international conference on engineering design (ICED) (pp. 13-20). Bury St Edmunds: Professional Engineering Publishing ltd.

Huet, G. 2004. "Design transaction monitoring and support for design rationale capture", Report for transfer to PhD, Department of Mechanical Engineering, University of Bath.

Husemann, P., Landkin, P.B., Sanders, J., Struphorn, J. 2003. "A WBA of the *Royal Majesty* Accident", RVS-RR-03-01, RVS Group, University of Bielefeld, 1 July 2003. Available

from www.rvs.uni-bielefeld.de.

Hutchins, E., Hollan, J.D., Norman, D.A. 1985. "Direct Manipulation Interfaces", *Human–Computer Interaction*, 1, 311-338.

Hutchins, E. 1995a. *Cognition in the wild*. Cambridge, MA: MIT Press.

Hutchins, E. 1995b. "How a cockpit remembers its speed", *Cognitive Science*, 19, 265-288.

Hutchins, E. 2000. “The cognitive consequences of patterns of information flow”, *Intellectica*, 30, 53-74.

Hutchins, E., Klausen, T. 1998 "Distributed cognition in the airline cockpit." In Y. Engestrom and D. Middleton (Eds) *Cognition and Communication at Work*. Cambridge University Press., 15-34.

Johnson, C.W. 2000. “Proving properties of accidents”, *Reliability Engineering and System Safety*, 67, 175–191.

Johnson, C.W. 2003. *Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting*. Glasgow, Scotland University of Glasgow Press (available at http://www.dcs.gla.ac.uk/~johnson/book/).

Johnson, C.W., Holloway, C.M. 2004. “‘Systemic Failures’ and ‘Human Error’ in Canadian TSB Aviation Reports Between 1996 and 2002”, International Conference on Human-Computer Interaction in Aeronautics (HCI-Aero 2004), Toulouse, France, 29 September–1 October, 2004.

Johnson, C.W. 2005. “V2 Using Violation and Vulnerability analysis to understand and the Root-Causes of Complex Security Incidents”, 2nd Workshop on Complexity in Design, Glasgow, UK, 10-12 March 2005 (available at http://www.dcs.gla.ac.uk/~johnson/book/).

Jun, G. C. 2007. “Design for patient safety: A systematic evaluation of process modelling approaches for healthcare system safety improvement”, PhD thesis, Engineering Department, University of Cambridge.

Kim, S., Alani, H., Hall, W., Lewis, P. H., Millard D. E., Shadbolt, N. R. and Weal, M. J., 2002.“Artequakt: Generating Tailored Biographies with Automatically Annotated Fragments from the Web”, Proceedings of the Workshop on the Semantic Authoring, Annotation & Knowledge Markup conjunction with the ECAI, France.

Kletz, T. 1994. *Learning from accidents*. 2nd Edition. Oxford, UK: Butterworth-Heinemann.

Koubek, R.J., Benysh, D., Buck, M., Harvey, C.M., Reynolds, M. 2003. “The development of a theoretical framework and design tool for process usability assessment.”, *Ergonomics*, 46:1-3, 220-242.

Kozak, M. 2003. “IT Project lessons from Titanic”,
(available in http//www.gantthead.com/article/).

Kushniruk, A., Triola, B., Borycki, E., Stein, B.,Kannry, J. 2005. “Technology Induced

Error and Usability: The Relationship between Usability Problems and Prescription Errors when using a handheld application", *International Journal of Medical Informatics*, 74:7-8, 519-526.

Lee, J. 1997. "Design rationale systems: Understanding the issues", IEEE Expert Vol. 12, No.13, pp.78-85.

Levenson, N.G., Turner, C.S. 1993. "An investigation of the Therac-25 accidents", IEEE Computer, 26(7):18-41, July 1993.

Levenson, N.G, 2004, "A New Accident Model for Engineering. Safer Systems," Safety Science, 42(4), pp. 23-270.

Liou Y., 1990. "Knowledge acquisition: issues, techniques, and methodology", Proc. of the 1990 ACM SIGBDP Conference on Trends and Directions in Expert Systems, SIGBDP '90. ACM Press, New York, NY, 212-236.

Livingston, A.D., Jackson, G., Priestley, K. 2001. "Root causes analysis: Literature review", prepared by WS Atkins Consultants Ltd for the Health and Saftey Executive, London.

Lützhöft, M.H., Dekker, S.W. 2002. "On your watch: automation on the bridge", *The Journal of Navigation*, 55, 83-96.

Mach, E. 1905. *Knowledge and error*. Dordrecht, The Netherlands: Dreidel. (English translation, 1976)

Marais, K., Dulac, N., & Leveson, N. 2004. Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems, ESD Symposium, Cambridge, MA, Massachusetts Institute of Technology.

McCall, R. J. 1991, PHI: a conceptual foundation for design hypermedia Design Studies, Volume 12, Issue 1, January 1991, Pages 30-41

McElroy, M.W. 2003. *The new knowledge management: Complexity, learning, and sustainable innovation*. KMCI Press/Butterworth-Heinemann, Burlington, MA.

McMahon, C., Lowe, A., Culley, S. 2004. "Knowledge management in engineering design: personalization and codification", *Journal of Engineering Design*, 15:4, 307-325.

Meister, D. 1971. *Human factors: Theory and factors*, New York: Wiley.

Miller, G.A. 1956. "The magical number seven, plus or minus two: Some limits of our capacity for processing information", *Psychological Review*, 63, 81-97.

Milton, N., Shadbolt, N., Cottam, H., and Hammersley, M., 1999. "Towards a Knowledge Technology for Knowledge Management", *International Journal of Human–Computer Studies*, 51, 615-641.

Mizoguchi, R., Ikeda, M., Seta, K., et al. 1995. Ontology for Modeling the World from Problem Solving Perspectives Proc. of IJCAI-95 Workshop on Basic Ontological Issues in Knowledge Sharing, pp. 1-12, 1995.

Mizoguchi, R., Ikeda, M. 1996. "Towards Ontology Engineering". Technical Report AI-TR-96-1, I.S.I.R., Osaka University, Japan.

Modern Power Systems, 2003. "FirstEnergy take major share of the blame", Modern Power Systems Journal, Vol. 23 Issue 11, p. 3. November 2003.

Muir, B.M., Moray, N. 1994. "Trust in automation: Part 1- Theoretical issues on the study of trust and human intervention in automated systems", *Ergonomics*, 37, 1905-1923.

Neisser, U. 1976. *Cognition and reality*. San Francisco, CA: Freeman.

Nonaka, I., Takeuchi, H. 1995. *The Knowledge-Creating Company*. New York: Oxford University Press, 1995.

Norman, D.A. 1981. "Categorization of action slips". *Psychological Review*, 88, 1-15.

Norman, D.A. 1992. "Design principles for cognitive artefacts", *Research in Engineering Design*, 4, 43-50.

Norman, D.A. 1993. *Things that Make Us Smart: Defending Human Attributes in the Age of the Machine*.. Reading, MA: Addison Wesley.

Norman, D.A. 1998. *The design of everyday things*. The MIT Press.

Norman, D.A. 2004. *Emotional design: Why we love (or hate) everyday things*. New York: Basic Books.

Noyes, J. M. 2004. "The human factors toolkit". In Human factors for engineers edited by C. Sandom & R. S. Harvey (pp. 57-79). London: IEE.

Noy, N. F., Fergerson, R. W., & Musen, M. A.., 2000. The knowledge model of Protege-2000: Combining interoperability and flexibility. In Proceedings of the 12th international conference on knowledge engineering and knowledge management (EKAW'2000), France.

Noy, N., McGuinness, D. 2003. "Ontology Development 101: A Guide to Creating Your First Ontology", Stanford University, CA (available at

http://protege.stanford.edu/publications/ontology_development).

Nunes, A., Laursen, T., 2004, Identifying the factors that led to the Ueberlingen mid-air collision: implications for overall system safety. Proceedings of the 48th Annual Chapter Meeting of the Human Factors and Ergonomics Society, September 20 - 24, 2004, New Orleans, LA, USA.

O'Hara, K., Shadbolt, N.R., Van Heijst, G. 1998. "Generalised Directive Models: Integrating Model Development and Knowledge Acquisition". *International Journal of Human–Computer Studies*, 49, 497-522.

Outhwaite, W., 1987. "*New Philosophies of Social Science: Realism, hermeneutics and critical theory"*. London: Basingstoke .Macmillan.

Parasuraman, R., Sheridan, T. B., Wickens, C. D. 2000. "A model for types and levels of human interaction with automation". *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans*, 30, 286-297.

Patil, R. S., Fikes, R. E., Patel-Schneider, P. E., McKay, D., Finin, T., Gruber, T. R., Neches, R., 1992. "The DARPA knowledge sharing effort: Progress report". In Rich, C., Nebel, B., Swartout, W., eds., Principles of knowledge representation and reasoning: Proceedings of the third international conference, Morgan Kaufmann.

Peltzman, S. 1975. "The effects of automobile safety regulation", *Journal of Political Economy*, Vol. 83, 4 August, 677-725.

Perrow, C.A. 1983. "The organizational context of human factors engineering". *Administrative Science Quarterly*, 28, 521-541.

Perrow, C. 1984. *Normal accidents*. New York: Basic Books.

Petroski, H. 1985. *To engineer is human: The role of failure in successful design*. New York, NY: St Martin's Press.

Petroski, H. 1994. *Design paradigms: Case histories of error and judgement in engineering*. Cambridge University Press.

Polanyi, M. 1966. *The Tacit Dimension.* London: Routledge and Kegan Paul.

Poli, R. 2002. "Ontological methodology", *International Journal of Human–Computer Studies*, 56, 639-664.

Preece, A., Flett, A., Sleeman, D., Curry, D., Meany, M., Perry, P. 2001. "Better Knowledge Management through Knowledge Engineering", IEEE Intelligent System. iJanuary. 60-72.

Prinzel, L.J. 2002. The relationship of self-efficacy and complacency in pilot-automation interaction. Langley Research Center: Hampton, VA: National Aeronautics and Space Administration. NASA/TM-2002-211925.

Ramesh, B., Dhar, V. 1992. "Supporting Systems-Development by Capturing Deliberations During Requirements Engineering", *IEEE Transactions on Software Engineering*, 18:6, 498-510.

Rasmussen, J. 1983. "Skills, rules, knowledge: signals, signs and symbols and other distinctions in human performance models", *IEEE Transactions on Systems, Man, and Cybernetics, SMC-13*, 257-267.

Rasmussen, J. 1985. "Trends in human reliability analysis", *Ergonomics*, 28:8, 1185-1195.

Rasmussen, J. 1986. *Information processing and human-machine interaction: An approach to cognitive engineering.* London: Elsevier.

Rasmussen, J. 1987. "Mental models and the control of action in complex environments", *Informatics and Psychology Workshop*, 41-69.

Rasmussen, J. 1999. "Ecological interface design for reliable human-machine systems", *The International Journal of Aviation Psychology*, 9:3, 203-223.

Reason, J. 1990. *Human error*. Cambridge University Press,

Reason, J. 1997. *Managing the risks of organisational accidents*. Aldershot, UK: Ashgate.

Ritzer, G., Zhao, S. & Murphy, J. 2001. "Metatheorizing in sociology: The basic parameters and the potential contributions of postmodernism. In: Turner, J (ed.) Handbook of Sociological Theory. Kluwer, New York, pp. 113 – 131.

Roberts, K.H. 1988. *Some characteristics of high reliability organizations*. Berkeley, CA: Center for Research in Management, University of California, Berkeley Business School.

Rochlin, G.I. 1999. "Safe operation as a social construct", *Ergonomics*, 42:11, 1549-1560.

Rodrigo, L., Benjamins, V. R., Contreras, J., Paton, D., Navarro, D., Salla, R., Blazquez, M., Tena, P., Martos, I., 2005. "A Semantic Search Engine for the International Relation Section", Proceedings of the ISWC 2005.

Russel, D.M., Maglio, P.P., Dordick, R., Neti, C. 2003 *Dealing with ghosts: Managing*

the user experience of automic computing., IBM Systems Journal, Volume 42 , Issue 1 (January 2003), 177 – 188.

Salmon, P.M., Stanton, N.A., Young, M.S., Harris, D., Demagalski, J.M., Marshall, A., Waldmann, T., Dekker, S. 2003. "Predicting Design Induced Pilot Error: A comparison of SHERPA, Human Error HAZOP, HEIST and HET, a newly developed aviation specific HEI method". In D. Harris, V. Duffy, M. Smith and C. Stephandis (Eds.) *Human Centred Computing*. Mahwah, NJ: Lawrence Erlbaum Associates, 567-571. ISBN: 0 8058 4932-7.

Samuel, A., Weir, J. 2000. *Introduction to engineering design modelling, synthesis and problem solving strategies*, Chippenham and Reading, UK: Antony Rowe Ltd.

Sanders, J., McCormick, E.J. 1993. *Human factors in engineering and design*. 7th Edition, London: McGraw Hill.

Sarter, N.B., Woods, D.D. 1995. "How in the world did we ever get into that mode? Mode error and awareness in supervisory control", *Human Factors*, 37:1, 5-19.

Sarter, N.B., Woods, D.D., Billings, C.E. 1997. "Automation surprises", in G. Salvendy (Ed.) *Handbook of Human Factors & Ergonomics*, second edition, Wiley. pp. 1926-1943.

Schreiber, G., Akkermans, H., Anjewierden, A., de Hoog, R., Shadbolt, N., Van de Velde, W. and Wielinga, B. 1999. Knowledge Engineering and Management: The CommonKADS Methodology, MIT Press.

Schreiber, G., De Hoog, R., Akkermans, H., Anjewierden, A., Shadbolt, N., de Velde, W.V. 2000. *Knowledge Engineering and Management: The CommonKADS Methodology*. MIT Press, Cambridge, MA, ISBN: 0262193000.

Scott, A.C., Clayton, J. E., Gibson, E., 1991, A Practical Guide to Knowledge Acquisition, 1st. ed., Addison-Wesley.

Selbig, J. 1987. "Knowledge acquisition by inductive learning from examples". International Workshop All '86 on Analogical and inductive inference, p.145-163, January 1987, Wendisch-Rietz, Germany

Senders J, Moray N, 1991, Human Error. Erlbaum, Hillsdale NJ.

Shadbolt, N., Milton, N. 1999. "From Knowledge Engineering to Knowledge Management". *British Journal of Management*, 10, 309-322.

Shapiro, D. 1994. "The limits of ethnography: Combining social sciences for CSCW".

Proceedings of Computer supported cooperative work (CSCW), 94, 417-428. New York.

Sheridan, T.B. 1987. "Supervisory control". In G. Salvendy (Ed.) *Handbook of human factors*. New York: John Wiley & Sons.

Smith, B., 2003. "Ontology". Preprint version of chapter "Ontology", in L. Floridi (Ed.), *Blackwell Guide to the Philosophy of Computing and Information*. Oxford: Blackwell. 155–166. (http://ontology.buffalo.edu/smith/articles/ontology_pic.pdf)

Stanton, N.A., Baberm, C. 2002. "Error by design: methods for predicting device usability", *Design Studies*, 23, 363-384.

Stokes, M. (Ed.), 2001. Managing Engineering Knowledge; MOKA: Methodology for Knowledge Based Engineering Applications. Professional Engineering Publishing, London.

Streff, F.M., Geller, E.S. 1998. "An experimental test of risk compensation: between-subject versus within-subject analyses", *Accident Analysis and Prevention*, 20, 277-287.

Svendung, I., Rasmussen, J., 2002."Graphic representation of accident scenarios: mapping system structure and the causation of accidents". Safety Science, vol. 40, pp. 397-417.

Sweet, W., Spectrum, 1995 "Glass cockpit", IEEE, Volume 32, Issue 9, Sep 1995, Page(s):30 – 38.

Turner, B.T. 1977. "Senior Clayton Fellowship Final report: Information for engineering design work", London: The Institute of Mechanical Engineers.

Ugwu, O.O., Anumba, C.J., Thorpe, A. 2001. "Ontology development for agent-based collaborative design", *Engineering, Construction and Architectural Management*, 8(3), 211-224.

Uschold, M., Gruninger M. 1996. "Ontologies: Principles, Methods, and Applications", *Knowledge Engineering Review*, 11, 96-137.

Vicente, K.J., Rasmussen J. 1992. "Ecological interface design: theoretical foundation", *Systems, Man, and Cybernetics*, 22, 589-606.

Wagner, W.P. 1990. " Issues in knowledge acquisition ", September 1990 SIGBDP '90: Proceedings of the 1990 ACM SIGBDP conference on Trends and directions in expert systems, Publisher: ACM

Wagenaar, W.A., Hudson P.T., Reason J.T. 1990. "Cognitive failures and accidents", *Applied Cognitive Psychology*, 4, 273-294.

Wichansky, A.M. 2000. "Usability testing in 2000 and beyond". *Ergonomics*, 43:7, 998-1007.

Wiegmann, D., Shappell, S. 2003. A human error approach to aviation accident analysis: The human factors analysis and classification system. Aldershot, Great Britain: Ashgate Publishing Company.

Wielinga, B., Sandberg, J., Schreiber, G. 1997. "Methods and Techniques for Knowledge Management: What has Knowledge Engineering to Offer?" *Expert Systems with Applications*, 13:1, 73-84.

Wiener, E.L. 1988. "Cockpit automation", In E.L. Wiener and D.C. Nagel (Eds), *Human Factors in Aviation*, San Diego, CA: Academic Press.

Wilde, G.J.S. 1982. "The theory of risk homeostasis: Implications for safety and health", *Risk Analysis*, 2, 209-225.

Wilde, G.J.S., Gerszke, D. and Paulozza, L., 1998. Risk optimization training and transfer. Transportation Research Part F: Traffic Psychology and Behaviour, 1, 77-93.

Woods, D.D., Cook, R.I. 1999. "Perspectives on Human Error: Hindsight Bias and Local Rationality". In F. Durso (Ed.) *Handbook of Applied Cognitive Psychology*. New York: Wiley, 141-171.

Woods, D.D. 2000. "Behind Human Error: Human factors research to improve patient safety", American Psychological Association (available at http://www.apa.org/ppo/issues/ shumfactors2.html).

Zhang, J. 1992. "Distributed Representations: The Interaction between Internal and External Information". PhD Dissertation, University of San Diego, CA.

Bibliography of accident reports

AAIB, 1990. "Report on the accident to Boeing 737-400, G-0 Brie near Kegworth Leicestershire on January 8th 1989", Air Accidents Investigation Branch, Department for Transport, Aircraft Accident Report 4/90, London, HMSO.

AAIB, 1994., "Boeing 747-243, N33021, at London Gatwick Airport, on 7 February 1993", Air Accidents Investigation Branch, Department for Transport, Aircraft Incident Report 4/94, London, HMSO.

AAIB, 1997. "Report on the accident to Aerospatiale AS 355F1 Twin Squirrel, G-CFLT Near Middlewich, Cheshire on 22 October 1996", Air Accident Investigation Branch, Department for Transport, Aircraft Accident Report 4/97 (EW/C96/10/8), London, HMSO.

Aviation Safety Network, 1988. "Accident of McDonnell Douglas DC-9-82 Northwest Airlines, 16 August, 1987" (available in http://aviation-safety.net/database/record.php?id=19870816-2).

Aviation Safety Network, 1988. "Accident of Airbus A300B2-203 Iran Air, 3 July, 1988" (available in http://aviation-safety.net/database/record.php?id=19880703-0).

Aviation Safety Network, 1990. "Accident of Airbus A.320-230 Indian Airlines, 14 February, 1990" (available in http://aviation-safety.net/database/1990/900214-2.htm).

Aviation Safety Network, 1992. "Accident of Airbus A 320, January 20, 1992" (available in http://aviation-safety.net/database/1992/920120-0.htm).

Aviation Safety Network, 1994a. "Accident of British Aerospace 4101, January 7, 1994" (available in http://aviation-safety.net/database/1994/940107-0.htm).

Aviation Safety Network, 1994b. "Accident of Airbus A 300, April 26, 1994" (available in http://aviation-safety.net/database/1994/940426-0.htm).

Aviation Safety Network, 1995. "Accident of American Airlines, December 20, 1995" (available in http://aviation-safety.net/database/1995/951220-1.htm).

Aviation Safety Network, 2002. "Midair collision of Boeing B757-200 and Tupolev 154M, July 1, 2002" (available in http://aviation-safety.net/database/record.php?id=20020701-0).

Aviation Safety Network, 2005. "Accident of Boeing 737-300, August 14, 2005" (available in http://aviation-safety.net/database/record.php?id=20050814-0).

ATSB, Aviation Safety Investigation Report, 1999, "Accident of Super King Air 200, 21 June 1999: occurrence number 199902928" (available in http://www.atsb.gov.au/publications/investigation_reports/1999/AAIR/aair199902928.aspx).

ATSB, Aviation Safety Investigation Report, 2000, "Accident of Beech Super King Air 200 aircraft, 04 September 2000: 200003771" (available in http://www.atsb.gov.au/publications/investigation_reports/2000/AAIR/aair200003771.aspx).

Bundesstelle für Flugunfalluntersuchung, Untersuchungsbericht, AX001-1-2/02 Mai 2004, "Midair collision of Boeing B757-200 and Tupolev 154M, July 1, 2002"

CHA, 2000. "Methotrexate toxicity, An inquiry into the death of a Cambridgeshire patient in April 2000", Cambridge, UK: Cambridgeshire Health Authority.

HSE, 2000. "The train collision at Ladbroke Grove 5 October 1999. A report of the HSE investigation". Health and Safety Executive. London:HMSO.

NTSB, 1995. "Grounding of the Panamanian Passenger Ship *Royal Majesty* on Rose and Crown Shoal near Nantucket, Massachusetts", National Transportation Safety Board, Marine Accident Report, Number NTSB/MAR-97/01.

NTSB, 2002. "Aircraft Accident Report: Loss of control and Impact with Pacific Ocean, Alaska Airlines Flight 261, McDonnell Douglas MD-83, N963AS, about 2.7 Miles North of Anacapa Island, California, January 31, 2000", National Transportation Safety Board, Aviation Accident Report, Number: AAR-02-01

NTSB, 2003. "Collision of Burlington Northern Santa Fe Railway in Scottsbluff, Nebraska, February 13, 2003", National Transportation Safety Board, Accident No.: DCA-03-FR-003 (http://www.ntsb.gov/publictn/2004/RAB0402.pdf).

US Nuclear Regulatory Commission, 2003. "Fact Sheet on the Accident at the Chernobyl Nuclear Power Plant", Last revised 23 June, 2003 (http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/chernobyl-bg.html).

US Nuclear Regulatory Commission, "Fact Sheet on the Accident at Three Mile Island", Last revised 1 March, 2004 (http://www.tmia.com/accident/NRCFactSheet.pdf).

US Senate Inquiry report, 1912. "Titanic disaster report", The Committee on Commerce of the United States Senate, RES. 283, e 12, (available from the "Titanic

inquiry project", at www.titanicinquiry.org/USInq/USReport/).

US-Canada Power System Outage Task Force, 2004. "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations", Ministry of Energy, April 2004 (available in https://reports.energy.gov/BlackoutFinal-Web.pdf).

APPENDICES

APPENDIX A: CLASSIFICATION OF CATEGORIES USED IN DATA SET OF THE CASE STUDY (ACCIDENT REPORTS IN THE AUSTRALIAN AVIATION ACCIDENT REPORT SYSTEM)

① description of the accident (occurrence number, date of accident, time of accident, accident type, cause of failure, failed system, defective artefact, failing system, improvement of system, design feature, types of operation at the accident, critical circumstance, trust in system)

② people involved in the accident (pilot in command, co-worker, controller, maintenance staff, other people)

③ condition in operation (start-up or preparation, during operation, changing mode, landing emergency)

④ state of mind of operators (normal, high work-load, complexity, time constraint, simultaneous work, failure of part of the system, abnormal external factor)

⑤ failed systems: system failures (display, gauge instrument, switches, internal system, managing devices, communication system, planning, space/view/location)

⑥ failed design: design failures (identifying a state of the system, location of target, procedure, protective measure, operation, what to do next)

⑦ causes of the error (different possibility, hiding important property, confusing with amount of information, confusing with case of information, providing unreliable information, conflict with previous experience, difficult to deal with the artefact, not providing relevant information, too much reliance on the system, difficult to distinguish, providing a method unfriendly or less used than before, making it easy to do or access a wrong way in using the artefact)

⑧ error types (misreading, miswriting, misinterpretation, misunderstanding, did not recognise, inattentional activity or automation mode, inappropriate performance, not following sign, not monitoring, violation of rules or procedures, not doing, not checking, difficult to understand, forgot to do)

⑨ theory (gulf of execution/evaluation, plan delegation, design affordance, irony of automation (inability), irony of automation (monitoring failure), trust in automation, automation surprise, risk homeostasis)

⑩ cause of accident (mechanical failure, operator failure, external factors, unknown)

APPENDIX B: LIST OF ACCIDENTS OF FAILED SYSTEMS INVOLVED IN HUMAN ERROR (CASE STUDY IN SECTION 5.2)

occurrence number	System/artefact/process
200403722	runway
200404285	wire detection system
200205901	Windsock
200100596	weight unit conversions (pounds to kilograms) procedure
200201228	weather radar display
199902928	warning system, bleed air switches
199503057	V1 cut procedure
200105618	turbine engine
199903790	traffic information for conflicting traffic
200203094	traffic communication system, non-standard route
199905438	traffic communication system, lateral separation
200004082	traffic communication system, flight strip
199901012	traffic communication system
199901070	traffic communication system
200004880	traffic communication system
199904312	traffic communication system
199902511	traffic communication system
199903436	traffic communication system
199804135	traffic communication system
199902459	traffic communication system
199904771	traffic communication system
200401273	traffic communication system
200202709	traffic communication system
200104881	traffic communication system
199905466	traffic communication system
199805078	traffic communication system
199802472	traffic communication system
200102905	traffic communication system
199800870	traffic communication system
199901959	traffic communication system
200402065	traffic communication system
200201846	traffic communication system
199905463	traffic communication system
199902458	traffic communication system
199805323	traffic communication system
199801905	traffic communication system
199804856	traffic communication system
200102139	traffic communication system
199804984	traffic communication system

occurrence number	System/artefact/process
200004882	traffic communication system
200203449	traffic communication system
200004709	traffic communication system
200106230	traffic communication system
199802964	traffic communication system
200402622	traffic communication system
200005295	traffic communication system
200305235	traffic communication system
199804849	traffic communication system
200201725	traffic communication system
199903768	traffic communication system
199904284	traffic communication system
200002379	traffic communication system
200403800	traffic communication system
200402714	traffic communication system
200202896	traffic communication system
200205540	traffic communication system
199902014	traffic communication system
199903590	traffic communication system
199900970	traffic communication system
200105942	traffic communication system
200100135	traffic communication system
199702768	traffic communication system
200006013	traffic communication system
200003093	traffic communication system
200101996	traffic communication system
199903602	traffic communication system
200100889	traffic communication system
200103344	traffic communication system
200002485	traffic communication system
200401411	traffic communication system
199702957	traffic communication system
200002060	traffic communication system
200003847	traffic communication system
200003594	traffic communication system
200103164	traffic communication system
200101080	traffic communication system
200105559	traffic communication system
199902415	traffic communication system
199901401	traffic communication system
200000869	traffic communication system
199902001	traffic communication system
199803437	traffic communication system

occurrence number	System/artefact/process
199900192	traffic communication system
199701423	traffic communication system
200302403	traffic communication system
200003793	traffic communication system
199802135	traffic communication system
199900844	traffic communication system
200104280	Traffic collision alert system(TCAS)
200005030	thrust lever position
199802755	the positioning of the controller pilot data link
200004914	the air situation display
199903711	TCAS
199902114	taxiway visibility
199900153	taxiway system, runway sign
200103240	taxing speed
199802817	taxing after landing
200401661	takeoff weight
199502837	takeoff weight
199900833	takeoff technique
199905168	TAAATS
199805341	TAAATS
199600094	steep clime after takeoff
199805068	stall warning system
199905121	spatially disorientated
199904842	spatially disorientation
200003233	spatial disorientation, darkness
199700052	SODPROPS
200300894	separation between aircrafts
199703150	navigation system
200303726	runway entrance
200003862	runway indicator
200102695	runway entrance
200103433	runway entering
200403720	runway entrance
199803910	runway control, runway selection button, flight pr
199804072	runway
200202710	runway
200104399	radio altimeter antenna
199902615	radar display
200002644	propeller RPM indication
199900645	power line cable detection
200004186	power lines
200400437	power line
199905026	power line

occurrence number	System/artefact/process
200201723	power line
200100252	power line
200401181	power line
200000868	power line
200402949	power line
200404286	power cable marks
200004914	positional information display system
199902679	nose landing gear
199805348	navigation/communication system
199805874	navigation system
199802022	mid-air collision preventing
199902550	mid-air collision preventing
199703850	mid air collision preventing
200003533	MEL procedure
200302433	MCDU, Flight management system(FMS)
200002899	low rotor RPM caution
200102455	loss of cabin pressurisation, select function ALT
200003293	loss f tail rotor effectiveness
200002693	load weight
200002989	load control
199902117	load
200003321	load
199800262	load
199904972	lateral separation diagrams
199903131	landing gear, flaps
200000148	landing gear warning
199403038	landing gear
200105698	landing gear
199701900	landing below the minimum altitude
200302037	landing gear, flaps/slats handle
199704041	landing gear
199902874	instrument landing system
200105743	inhibit switch, landing gear failure
200404460	hypoxic
200003951	hypoxia
199803921	holding pattern
199802757	GPS arrival
199805603	fuel type error
200102253	fuel tank filler cap unlock
200200885	fuel system
200001827	fuel selector system, operation manual
200402049	fuel selection, emergency restart producer
199403314	fuel selection system

occurrence number	System/artefact/process
200001434	fuel quantity system
199702841	fuel quantity system
200002018	fuel quantity indication system
200000765	fuel quantity indication system
200003056	fuel quantity check, dipstick
200200047	fuel quantity check
199804432	fuel quantity checking system
200303599	fuel quantity
199702601	fuel quantity
200404700	fuel quantity
199905596	fuel quantity
200400265	fuel quantity
200100348	fuel management system
200403210	fuel management system
200402797	Flap/slat
200200007	fuel gauge system
199900820	fuel
200004806	flight progress strip management, traffic communication system
199702620	flight planning system, air traffic control strip
200401904	Flight Management Computer (FMC)
200402747	Flight Management Computer (FMC)
200200463	flight instruments
199901009	flight in adverse weather
199802529	flap 20 asymmetric approach
200000492	engine failure simulation
200400443	emergency power lever
200105715	emergency checklist
199800640	elevator input
199800442	dynamic rollover situation
200301435	door open warning display
200205307	donning of oxygen masks during emergency
200004671	donning of masks at emergency
200003725	don oxygen masks
200100443	detecting hazard of wire
200302172	descent below the MDA
200203074	de-ice, stall warning system, autopilot
200200094	CPDLC
200200190	CPDLC
199804129	controller-pilot data link communication, CPDLC
200402060	contamination of fuel
199804690	console, annotation of flight progress strips
199702691	console
199803972	conditional crossing clearance

occurrence number	System/artefact/process
200005967	communication, frequency selector gears
199902487	chart
200105351	Chart
200300008	cabin pressurisation
200105188	bleed air off warning system
199804069	blanket clearance
200203171	battery
200400856	Automatic terminal information system(CATIS)
199900990	APU
199501246	approach chart
200301990	altimeter
200302847	allowable take-off weight
200202385	air traffic control instructions
199902003	air traffic computer
200000933	Air Situation Display (ASD)
199804347	aerodrome chart

APPENDIX C: LIST OF ACCIDENTS USED FOR THE CASE STUDY AND ONTOLOGY DEVELOPMENT (CHAPTER 5 AND 7)

CASE NUMBER (OCCURRENCE NUMBER)	FORM OF HUMAN SYSTEM INTERACTION FAILURE
1 (199902928)	An aircraft entered into a depressurizing level of altitude without relevant action. The pilot in the aircraft failed to follow tack-off checklist actions. He did not finish operating GPS setting. He did not recognize the aircraft passing over a limited level and an alert sign of depressurizing. He inadvertently switched a vent fan switch instead of an engine bleed-air switch.
2 (199902003)	Two aircrafts conducted a consecutive departure. The superior performance of the later departure aircraft to that of the previous departure aircraft resulted in reducing separation. The controller did not recognise this difference while instructing.
3 (200105715)	While on climb through FL180, the copilot's two electronic flight information system (EFIS) screens on the right side of the aircraft's instrument panel failed. While the crew had consulted the EFIS failure/disturbances checklist, they failed to recognise the problem arose. They omitted the first item of a generator failure in the checklist.
4 (199702691)	Two aircrafts flied same level of altitude, and resulted in a breach of the collision avoidance limitation having received a traffic alert and collision avoidance system (TCAS) traffic advisory (TA). As the controller removed strips on the aircraft, they missed to instruction before the conflict occurred.
5 (200105351)	The crew of a Boeing 767 (B767) had been cleared to taxi for departure from runway 01, intersection "A7", at Brisbane. They proceeded along taxiway "B" then, incorrectly, initiated a turn onto taxiways "B5" and "A", which was in conflict with rapid exit taxiway "A5S".
6 (199805068)	Shortly after the aircraft entered the holding pattern it suffered an aerodynamic stall and rolled approximately 126 degrees to the left and pitched nose down to approximately 35 degrees. The pilot did not identify the possibility of aerodynamic stall before conducting the holding pattern.

7 (200201725)	An infringement of separation standards occurred 70 NM east of Darwin, NT, between a descending Boeing 737-376 (737) and an Embraer EMB-120 (Brasilia) that was maintaining level flight. The pilots misunderstood information from TCAS aural warning. They did not scan IVSI display.
8 (199805341)	Without notice, the display in the Brisbane Air Traffic Control Centre changed to an uncoupled black track without label data, resulting in the sector controller losing situational awareness. The controller deleted information on the computer display without checking.
9 (200402747)	The flight crew of a Boeing 737-838 aircraft, registered VH-VXF, received a terrain proximity caution from the aircraft's enhanced ground proximity warning system (EGPWS) while descending to the south-south-east of Canberra Airport. The crew inadvertently commanded the FMC to establish the aircraft in a wrong position in the FMC hold page.
10 (199702620)	As the B737 had reached FL300 before the crew received the instruction to descend, and as the vertical separation standard was 2,000 ft, an infringement of the separation standards had occurred. The controllers failed to identify correct time of passing a point and did not crosscheck the information.
11 (200004806)	As the Macchi climbed through 8,000 ft, while approximately 6 NM south of Williamtown, it passed within 1 NM of the C340. There was an infringement of separation standards. The sector controller failed to identify the location in the radar display system.
12 (200105188)	The pilot did not complete the Pre Take Off and After Take Off cabin pressurization checks. He did not recognize the illumination of warning light.
13 (199803972)	The controllers issued two aircrafts in cross runways. The operation of a conditional clearance for a taxiing aircraft to cross an active runway failed.
14 (199503057)	During V1 cut procedure at night, the aircraft struck a tree due to the loss of control. The pilot understood the V1 procedure was allowed.

15 (199804129)	The communication between air traffic controllers and flight crew via the controller-pilot data link communications (CPDLC) system was failed.
16 (199403314)	The right engine failed due to the mismanagement of the fuel system in the aircraft.
17 (20003725)	The plot in command did not don oxygen masks during the initial descent in order to avoid a pressurization problem.
18 (199804690)	The sector controllers failed to recognize conflict between two aircraft.
19 (199805078)	The crews of two aircraft were not acknowledged traffic information transmitted. As a result there was a conflict between two aircraft.
20 (199805874)	The pilot of search rescue aircraft inadvertently searched in the area assigned to the other rescue aircraft. The reconfiguration of GPS setting was not conducted.
21 (200001827)	The fuel selector valve did not position the valve to the right tank. The pilot failed to check balance of both fuel selections during the pre-flight check.
22 (199803921)	A pilot conduct a wrong holding pattern procedure without checking further information assuming it is right to apply a general rule which he had experienced before.
23 (199803910)	Two aircrafts landed and departed at a same runway at a same time. Both the aerodrome controller and the surface movement controller issued to land and to depart for two airplanes at the same time.
24 (199900153)	The crew interpreted taxiway G3 to be taxiway Y on the basis of that information. The crew subsequently turned the aircraft onto taxiway G3, which was closed.
25 (199804432)	The engines had stopped because of fuel exhaustion. The pilot did not correctly check fuel quantity before the flight.
26 (200200047)	The right engine failed due to insufficient fuel in the right tank while the aircraft was in a climb attitude. The pilot did not correctly check fuel quantity before the flight.

27 (200400856)	During the ILS Glide path approach the aircraft commenced to descend bellow the limited ground level. The controller was unaware that only the localiser was available. The controller did not recognise the limitation of information displayed in the Computerised Automatic Terminal Information System (CATIS).
28 (199802755)	Five minutes prior to reaching LEMIB the crew of the B767 received a traffic alert and collision avoidance system traffic advisory warning. There was other aircraft within the separation standard. There was distraction and subsequent failure of the sector controller to regularly scanning the flight progress strips.
29 (200105743)	When the flight crew was preparing for landing, the main landing gear failed to extend following normal selection. When the flight crew selected the landing gear to the down position (extended), the landing gear inhibit switch was in the INHIBIT position, thereby preventing normal extension. When the flight crew prepared the aircraft for flight, they did not confirm the position of the main landing gear inhibit switch.
30 (200003533)	The aircraft pressurisation and airconditioning systems automatically shut down, and the cabin pressure altitude began to increase. The aircraft departed with a minimum equipment list (MEL) in which restriction applied following the failure of the right engine high-pressure valve (HPV). The crew interpreted the operator's MEL to mean that at engine "idle thrust" they were to turn the bleed air from that engine to off.
31 (200100443)	A helicopter collided with wires and impacted the ground in a densely wooded area about 200 metres beyond the wires. The pilot did not identify the wire.
32 (200202385)	A Cessna 172 (Cessna) conflicted with a departing Boeing 747-300 (B747) while the B747 was climbing through the altitude of the Cessna. The aerodrome controller issued the pilot of the Cessna with a clearance to track via the 'southern shores' intending the 'southern shores of Trinity Inlet'. However, the pilot of Cessna wrongly understood the term as the shoreline on the southern side of Cairns airport (which was the northern shore of the Cairns harbour).

33 (200400443)	While conducting an in-flight familiarization of advancing the emergency power lever (EPL) to simulate manual introduction of fuel to the engine, there were high engine temperature. The engine ignition switch was not in the ON position during the initial operation of the EPL during this training. The pilot understood the procedure is acceptable.
34 (200302433)	During the final approach, there was missed approach due to the aircrafts' intercepting wrong altitude. The altitude constraint in the flight plan (in FMS) for the inbound turn was replaced by the (lower) altitude constraint for the next flight segment. The pilots did not identify their wrong data input to the FMS.
35 (200104280)	A Boeing 767-336 (B767) was on final approach to runway 27 at Melbourne and passing 1,400 ft on descent, when the crew received a Traffic Alert and Collision Avoidance System (TCAS) traffic advisory (TA) with an aircraft 600 ft below. The pilot did not aware of inoperability of transponders for five minutes warm-up.
36 (199900192)	The crew of the Fokker was conducting the overshoot onto a radar heading which placed the aircraft in close proximity to the Cessna. The approach controller issued the overshoot instruction without reference to the departure controller.
37 (200200007)	The left engine low oil pressure and generator warning lights had illuminated. The aircraft's engines failed due to fuel exhaustion. The pilot did not correctly check the fuel quantity before the departure.
38 (200200094)	Another aircraft that was on a reciprocal track at the same level of OEB. The vertical distance between OED and OEB reduced to 800 ft, and to 700 ft between OED and the third aircraft. There was an infringement of separation standards. The controller sent a wrong pre-formatted message to the crew of OEB through CPDLC.
39 (200201228)	After setting course for Canberra, the conditions suddenly became dark, associated with an increase in the turbulence level and rain intensity. The aircraft was inadvertently flown into an area of severe convective weather activity. The flight crew misinterpreted the depicted weather radar returns.

40 (200200190)	There was an infringement of separation standards. The controller prepared the message in advance. The controller intended to send the message to the crew of the north-east bound B747 once they had passed the south-west bound B747 and a separation standard had been established. However, he unintentionally sent the message before the two aircraft had passed.
41 (200200463)	As the aircraft approached each other 12 NM east of Sydney, an infringement of the radar separation standard occurred. After take-off, the B737 entered cloud and encountered turbulence. The pilot in command was observing the weather situation and did not monitor the flight instruments as the aircraft approached the assigned altitude.
42 (200301990)	As the aircraft approached 500 ft above ground level, the rate of descent was assessed as too high and the first officer called for a missed approach to be conducted. The aircraft’s altitude was high because the barometric settings on the altimeters had not been set to the airfield QNH of 1028 hectopascals (hPa) but rather had been left on 1013 hPa.
43 (200003056)	After departed on a 30-minute scenic flight, the engine suddenly failed. Fuel exhaustion may have contributed to the engine's loss of power. The pilot made an error to assess fuel quantity check with a new fuel dipstick.
44 (199804072)	A vehicle was on the runway. At the time the landing clearance was issued, Car 23 was parked on the runway, approximately 200 m from the southern end. The aerodrome controller did not adequately scan the runway prior to issuing a landing clearance to the crew of WBA.
45 (199804069)	As the B737 approached the crossing point of runway 30 on taxiway Foxtrot 2, the crew saw the Pilatus commence to takeoff. The ADC and SMC did not conduct an effective scan of runway 30 or the flight progress strip display prior to clearing the Pilatus to take off.
46 (199902874)	Shortly after descent had been initiated, both pilots noticed the aircraft commence a right turn away from the centreline of the localiser. Both pilots incorrectly tuned the Cairns runway 33 localiser on 109.5 MHz instead of the runway 15 localiser on 109.9 MHz and subsequently

	misidentified the morse-code identifier.
47 (200000765)	The low fuel warning light began to flicker. A few moments later the engine began to run roughly. The pilot planned the flight using a fuel consumption rate that was significantly less than the actual consumption.
48 (200100596)	The fuel consumption was 230 kg per hour more than normal. The cargo had been re-weighed. The actual cargo weight was more than 3,400 kg greater than the weight stated on the manifest. The four pallets had been carried without changing weight unit from pound to kilogram.
49 (200403210)	At about 1,500 ft above ground level (AGL), the engine abruptly failed. The pilot applied an emergency engine restart procedure, but failed. The pilot's response to the engine failure was not consistent with the aircraft manufacturer's or the operator's emergency and abnormal checklist instructions.
50 (200106230)	When the B767 descended through FL326, vertical and horizontal separation between the B767 and the C500. There was an infringement of separation standards. The controller entered FL330 into The Australian Advanced Air Traffic System (TAAATS). He subsequently, and unintentionally, assigned the crew of the B767 descent to FL300.
51 (200302037)	Following a normal take-off the pilot in command (PIC), the handling pilot, called for the landing gear to be retracted. A short time later, he noticed an amber warning appear on the airspeed scale on his primary flight display (PFD) screen. The copilot retracting the flaps/slats instead of the landing gear.
52 (200402797)	An aircraft collided with terrain 34 km south-east of Benalla. The flight did not follow the usual route to Benalla, but diverted south along the coast before tracking to the northernmost initial approach waypoint BLAED of the Benalla Runway 26L GPS NPA. While tracking to BLAED the aircraft diverged between 3.5 and 4 degrees left, without the pilot being aware of the error.

APPENDIX D: IMPLICATED SYSTEMS OF THE CASES (SECTION 5.3)

FAILED ARTEFACT [CASE NUMBER]	IMPLICIT DESIGN CONCEPTS
Takeoff check lists [1]	All necessary itineraries could be included in the list that would be performed by operators without difficulty or error.
Operating of automatic level–up into a pressurizing zone [1]	Operators could recognize and response to a critical by continuously checking the current state of a system.
Alert systems [1]	Operators could recognize warning signals provided by a system. The operator will look for alerts at any time or any circumstance.
Array of functions/ artefact [2]	Operators would do a right selection (action) of an intended position.
The SWIFT 2 standard instrument departure [2]	The design of minimum departure separation standard could be achieved by controllers. The controllers will continuously monitor process of consecutive departure.
Performance of similar type' aircrafts [2]	It is not an essential thing to consider ways in which people can more easily recognize difference of performance between two aircraft types by e.g. changing a model number when designing enhancing performance of the same model of an aircraft. The controller recognizes the difference of performance ability of similar types of aircrafts with a provided specification paper.
Data input into the air traffic control computer [3]	Because the data entry job to a computer system is a minor task, that task could not hurt operators' decision ability.
The EFIS (electronic flight information system) failure/disturbances checklist [3]	The crew would check the EFIS failure/disturbances checklist step by step from first item to last one.
Generator failure warning system [3]	Although there is no alert, it can be easily identified by the operator that a starter generator fails because a generator failure causes a cut of electricity.
The air traffic controller consol [4]	The controller has enough memory capacity to remember all flight progress strips. Display space in a controller consol is not an essential but an additional artefact to support memory of controllers.
Charts installed in the	It will be useful for operating if a printing function is

computer system [5]	included in a cockpit computer system. The usability and distinguishable of the chart is not consideration of design.
Detecting ice deposit [6]	It is not necessary to provide a particular device to detect ice deposit because operators can detect degree of ice deposit and determine with their experience by the onsite inspection.
Aerodynamic warning system [6]	Operators will be careful to conduct a holding pattern while icing condition. Although there is no warning sign, the operator would check all situations before conducting.
Alert and instruction functions in TCAS (Traffic Collision Alert System) [7]	An audio and visual alert and instruction system in TCAS help pilots to identify the situation and follow the instruction for remedial measurement. The pilot would compare the information provided whether which information is true or fault.
Data cancellation in TAAATS (The Australian Advanced Air Traffic Control System) [8]	The operator will be careful to delete or cancel data in a computer system. An alert message in the display wills effective measure to prevent adverse performance of an operator.
Selecting a mode in FMC (Flight Management Computer) [9]	Providing various modes in a computer system will help operators to perform in different ways.
An air traffic control strip printing system [10]	Data available in the system would be formatted into the specification of the system.
A flight-planning system [10]	The flight planning system should include all necessary times. The different specifications between a system to a system could be identified by operators.
Crosscheck of controllers [10]	Each controller would check data, even the data were provided by a system (e.g. computers).
The surveillance radar (SURAD) [11]	The radar did not have identification labels or height information. The limitation of the radar could be compensated by coordination of a sector controller and approach controller.
After Take Off check [12]	The checklist would be completed within an allowed time. There is no delay in the procedure. The GPS setting task would not deter the performance of operators. The aircraft was allowed to climb above 10,000 ft in an unpressurised state.
The cabin altitude warning system [12]	The warning illumination would alert the operator by colour and lighting of the warning system.
A conditional clearance of a taxiing aircraft to cross an active runway [13]	A conditional clearance procedure takes advantage of crossing runways and saves the departure and arrival times. The controllers would be aware of all aircrafts in the crossing runways. The controllers would remember a conditional crossing clearance is pending.

A V1 cut procedure at night [14]	If a description of a procedure in a manual were not clearly permitted, an operator would not use the procedure.
The controller-pilot data link communications (CPDLC) system [15]	The computer system helps communication between air traffic controllers and flight crew. The operator would recognize the limitation of the function on the system.
frequency (HF) radio systems [15]	High frequency (HF) radio systems compensate the CPDLC system. The operator would use backup systems while using a main system.
The fuel system [16]	The modification of the design of the fuel selection system from previous models would be easily recognized by the operator.
Donning oxygen masks [17]	The crew would wear oxygen masks when the masks were deployed.
Sector console and flight progress strips [18]	When traffic levels are increased, it would be help to decrease the level of controller's task that if coordinators just put into the work.
A traffic information transmission system [19]	If a system provided more than one frequency, it would help controllers and pilots to communicate and not to miss transmission. Radio congestion is not a serious problem to hamper the communication and wrong understandings.
A search plan [20]	The re-tasking details could be passed verbally from staff in the control system to pilots in search activity because the message search altitude and adjacent search aircraft was provided prior to take-off.
A navigation system [20]	The pilot would understand limitations of the navigation system. The check and reconfiguration tasks could be achieved by conducing procedures designed in normal basis.
Fuel selector system [21]	The pilot would check balance of both fuel selections during the pre-flight check procedure. The design requirement specification on operating procedures of pilots to operate the fuel supply cross feed for 60 seconds to verify normal operation could be achieved. Also, pilots should ensure normal operation of the fuel valves by positioning the fuel selectors to the off position to observe a decrease in fuel flow.
A holding pattern procedure [22]	The pilot would check what is a relevant holding pattern by asking to air traffic controllers if he(she) did not find information in a chart at the cockpit system.
Terminal chart [22]	The pilot would distinguish the depiction of a holding pattern from other marks in the chart.
Flight management	A holding pattern is not so much important information

computer database [22]	to compulsory input into a flight management computer database. The information could be checked by pilots.
The runway 11/29 selector [23]	Controllers will push down the runway selector button on the system after scanning the runway.
The flight progress strip display [23]	Once a clearance issue was conducted the flight strip was no longer need.
The airfield layout [23]	Designers try to utilise a system in efficiency. The more complicate a runway layout, the more maximise usability of the airfield for departure and arrival. Although the increased complexity of runway layout, the runway selector system can prevent controllers from inadvertent selection causing conflict accidents.
Sydney terminal chart [24]	Pilots would read correctly and notice differences of letters in the chart.
Fuel quantity assessment systems [25]	Pilots would assess the fuel quantity by comparing two systems; a fuel indicator and a fuel log.
Fuel quantity assessment systems [26]	The pilot would establish the actual fuel quantity on board the aircraft prior to departure by comparing three fuel quantity systems.
The computerised automatic terminal information system (CATIS) [27]	Constraints of a system could be compensated by operators with using other systems. The operator would check additional information which was not provided by the system.
The controller pilot datalink and the sector 8 operating console [28]	The task of scanning controller pilot datalink is not a main task of controllers. Therefore there is no problem if remove the dedicated controller pilot datalink controller. Designers believed that a controller could adequately manage both the controller pilot datalink and the sector 8 position.
The landing gear inhibit switch [29]	When the flight crew prepared the aircraft for flight, they can easily fond the position of the main landing gear inhibit switch to be in the INHIBIT position or not.
Manuals of a minimum equipment list (MEL) [30]	MEL 36-11-07 was titled "Engine Bleed High Pressure Valve (HPV)" and was composed of two parts. Part (a) detailed the actions to be taken if the bleed-air system was considered to be inoperative, and indicated that the bleed-air system was to be isolated and not used. Part (b) detailed the actions to be taken if one HPV was inoperative, "locked closed". However, the intention of the MEL was that the bleed-air system from that engine could still be used except in specified circumstances. They expect that operators would understand the intention.
A wire strike protection system (WSPS) [31]	The pilot could be aware of wires while flying low. The installation of a wire strike protection system is not a compulsory design specification.

Reference terms [32]	The pilot as well controllers would be familiar with instruction terms which have been normally used in instruction.
The emergency power lever (EPL) to simulate manual The pilot's operating handbook (POH) [33]	As it is not expected that there will be an in-flight familiarization of the emergency power lever, the aircraft manufacturer only included requirements for an actual FCU malfunction. The POH did not address the engine control settings for training of this type. The pilot would understand that not to mention it is to prohibit conducting it.
The multi-function control and display unit (MCDU) of the Flight management system (FMS) [34]	The pilot would recognise incorrect data input in the flight management system and correct it. The automatic movement of screens in the computerised display unit of the flight management system would help operators to conduct a setting.
Transponders of a Traffic Alert and Collision Avoidance System (TCAS) [35]	The transponders could require up to five minutes warm-up prior to operation. The limitation of design could be achieved by operators. Operators would ensure the operation of transponders before a departure.
Utilises the Operational Data Information [36]	The use of Operational Data Information for coordination between units was accepted as a standard operating procedure. However, the tower controllers and the Terminal Control Area controllers would not only rely on the Operational Data Information be achieved coordination with other communication facilities. They understand limitations of the Operational Data Information containing only the radar label display.
The fuel quantity indicating system. [37]	There are three systems available for fuel quantity identification: visual inspection on fuel tanks, fuel quantity indicators, and a fuel log system. The use of separate methods to establish fuel quantity on board is substantially more reliable than relying on one system. The pilot would use separate methods and compare these systems in order to verify the real fuel quantity.
Controller-Pilot Data Link Communications (CPDLC) [38]	Messages were compiled and initiated either by the crew of the aircraft or by ATC and were, in this case, pre-formatted. The use of pre-formatted messages was 'intended to reduce the possibility of misinterpretation and ambiguity'.
Weather Radar [39]	The radar antenna transmitted microwave energy in the form of pulses, which, if reflected off precipitation ahead of the aircraft, would be returned to the antenna. There were four colour codes that were directly related to precipitation intensity, ranging from black (no precipitation), green (minimum detectable moisture), yellow (medium moisture level), to red (strong to extreme moisture level). However, heavy rainfall could reduce the ability of the weather radar to provide a complete picture of the weather ahead.

	The limitation of the radar in which would be understood by the flight crew.
Controller-Pilot Data Link Communications (CPDLC) [40]	Preparation of the CPDLC message in advance may assist controllers with workload management. The pre-format design can help operators to save time and to reduce their tasks.
Monitoring the aircraft's weather radar [41]	The aircraft's weather can help pilots to assess the meteorological conditions. The distraction of pilots is not consideration of weather radar design.
Cockpit displays for altimeter [42]	The pilot can do the required altimeter setting. The task could not be forgotten.
The calibrated dip stick [43]	The wooden dip stick had been calibrated to measure the fuel quantity when inserted almost vertically into the tank, without passing through the hole in the tank baffle. The pilot would be aware that this method for measuring the fuel quantity was only valid when using the original manufacturer's supplied dip stick.
Checking runways [44]	The controllers can conduct effect scanning on runway before issuing instructions. The designation system helps them to recognise runway situations.
Blanket clearance [45]	The blanket clearance allows aircraft to occupy or cross runway 30 without a specific clearance from the ADC. The use of a blanket clearance reduced the need for segmented taxi clearances. The ADC and SMC would coordinate each other.
Morse codes in the flight management computer [46]	The flight crew can identify morse-code in the flight management computer.
The fuel consumption checking systems [47]	A fuel gauge and engine instrumentation provided pilots with fuel flow information. Apart from this the only fuel consumption data provided to pilots was on a specification sheet published by the manufacturer of the helicopter. The pilot would check the actual fuel consumption by comparing two fuel consumption checking systems.
A Weight checking system [48]	The operator would check the weights recorded on the manifest with the loadsheet issued by Load Control. There is no need a further system to figure out conversion of weight. It is an easy task for operators to check the figures whether the figures had been converted or not.
Emergency and abnormal checklist instructions [49]	The aircraft manufacturer's emergency and abnormal checklist instruction design to the engine failure could be formulated in differently from procedures used in other types of aircraft systems. The pilots would deal with the procedure without confusing with the other procedures used in other types of aircrafts.

The Australian Advanced Air Traffic System (TAAATS) [50]	The TAAATS entry task could not distract the attention of a controller even if the controller had to involve other tasks (e.g. talking to pilots or other people) while doing the task.
The procedure of a flap/slats lever movement [51]	Although the procedures of the movement of flap/slats or landing gear levers is similar and associated, pilots could not be difficult to manage the two levers correctly because they are different shapes and positions.
The flight management system [52]	The automatic flight management system would help the pilot to reduce laborious tasks. The pilot would check and confirm information displayed in the computerised system.

APPENDIX E: FAILURE MODE OF THE CASES (SECTION 5.3)

FAILURE CASE	FAILURE MODE IN TERMS OF DIE
Incomplete takeoff check lists [1]	Many items were included into an after take-off checklist procedure without considering the fact that a task, in case of failure or difficulty of the parts of jobs, delay or confound with other tasks. This led to puzzling of operators when they encounter an uncontrolled condition.
Unrecognized level-up into a pressurizing zone [1]	There were many itineraries to conduct on take-off check lists. If a pilot had to do one task in labour intensive cognition. This led to distracting operators' focus on continuously checking current altitude.
Misidentified location of a switch [1]	Location of switches in similar shape but different functions plays an important role to the performance of operators. Many switches are similar shapes in near location. This led to unintended action while the operator was busy with other tasks.
Unnoticed alert system [1]	An automatic warning system should have alerted operators to recognize a hazard. But operators being in a state of distracted cognition due to other tasks could not response to a weak warning such as lighting or message in a screen display. This led to not recognizing.
Unrecognizing the performance ability of similar types of aircrafts [2]	The performance of the B737-400 series aircraft was superior to that of the B737-300 series aircraft. There was no effective process to check the different performance. That led to controller's considering that the aircraft were like types for the purposes of departure standard.
Monitoring failure due to data entry [3]	The approach/departure controller elected to input data to the air traffic computer during the departure sequence. They were labour intensive and diverted his attention for the air situation display. This led not to monitoring the departure process of two aircrafts.
The overlooked item in a failure checklist [3]	There is no alert system for a voltage failure, and the symptom of the failure looked like a display error. It might be a right decision that the voltage failure is not a cause of the warnings because cascade warning illuminations showed there was enough electricity in the system. That led the crew to overlooking the first item of the EFIS failure/disturbances checklist, which required a check of the generator voltage.
An incorrect clearance issue [4]	The configuration of the Sector 3 console provided insufficient space to adequately display all relevant flight progress strips. As a result, controllers had developed the habit of removing strips at the earliest opportunity, thereby creating the potential for vital information to be missed.
Computer based printed charts [5]	Computer based printed charts in small size is difficult for pilots to read correctly. That led to misidentifying a correct taxiway.

Misinterpreting ice deposit [6]	Without a clear prohibition standard, it is easy for human to ignore unclear evidences and then consider as normal as routine practices. This led to misidentify the ice deposit in wings.
Failure of alerting aerodynamic stall in icing condition [6]	Without alerting operators could not identify aerodynamic stall in advance.
Unrecognized alert messages [7]	It is possible that the crew may have misidentified the TCAS aural warning. Prompt action was required to resolve the apparent ambiguity and the crew may have been guided more by the aural warning than by the IVSI display. That may have been, at least in part, due to the limitations of the IVSI display, where a pilot may initially rely more on the aural alert. Compared with a TCAS IVSI display, traffic information that is displayed on an EFIS screen increases the crew's situational awareness. However, pilots are trained to use all the information at their disposal and an aural alert would be the trigger to look at the IVSI display immediately. Therefore if the green band of the IVSI was indicating a required rate of descent of 1200-1500 ft/min, then the correct procedure would be to disengage the autopilot and smoothly adjust the pitch to attain that rate of descent.
Misinterpreted an emergency instruction [7]	The reported `descent' advisory was actually a `reduce descent' advisory that was misunderstood by the crew. In a temporal decision making condition human cognitions reduce to capturing only parts of information. That may lead the misinterpretation of the instruction.
Unintentional cancellation of data in a computer system [8]	TAAATS displays a warning message requesting confirmation of the cancellation action when a controller deletes a flight data record for an aircraft. This message does not warn controllers that they do not have jurisdiction of the aircraft. Airservices Australia have proposed that the warning message for non-jurisdiction flight data records should be amended to alert controllers to the fact that coordination is required prior to deleting the record. The coordinator had assumed that an aircraft on the ground at Cairns was the aircraft displayed as airborne and consequently felt that it was unnecessary to check further prior to deleting the record.
Misidentified mode in a computer system [9]	Mode changes in a display are unnoticed without an alerting function. A recent incident has indicated that there may be some confusion relating to the function of the Leg Distance (LEG DIST) prompt of the B737 FMC Hold page. The Leg Distance prompt allows entry of the actual length of the inbound Leg of a holding pattern in nautical miles. It does not refer to a DME limit as depicted on a charted holding pattern. Additionally, beware that a Leg Distance entry will override a Leg Time value. By entering a leg distance of 14 NM, the crew inadvertently commanded the FMC to establish the aircraft in a holding pattern that would take the aircraft about 11 NM beyond the published holding pattern limit.

Misinterpreted chart [9]	The holding pattern limits published for CCK, did not contain the referenced DME identifier (Canberra) in the limit notes. The holding pattern Distance Measuring Equipment (DME) limit distance on the referenced instrument approach chart was misinterpreted by the crew. The crew did not detect that the DME distance referenced on the chart was based on the Canberra DME. The instrument approach chart did not contain the specific Canberra DME identifier in the CCK holding pattern limits.
Misinterpreted flight progress printing system [10]	There are different criteria or specifications of input data in the flight progress printing system of the air controller system and a flight-planning system in an airplane. That led to misinterpretation of the flight progress printing system.
Misunderstood flight plan [10]	The flight plan for the A320 contained a manoeuvring time for the aircraft prior to setting course. The air traffic control strip printing system was unable to allow for a discrete manoeuvring time in the strip preparation. The Melbourne Sector 4 controller did not conduct a crosscheck calculation on the flight progress strip notation for the A320's estimated time of arrival at SUBUM.
Unaccomplished crosscheck [10]	There are many computerised systems and processes that reliable in previous process before a crosschecking task. The data were based on radar observation and information of the computerised flight progress printing system receiving information of airplane systems. This led to negligence or relying on the previous data.
Not informed from the surveillance radar (SURAD) [11]	The SURAD did not have identification labels or height information and that limitation increased the workload on the controller. Although the interim radar display system (IRDS) that was used by the sector controller had labels and a Mode “C’ height reading capability, the Macchi was not equipped with a Mode “C’ capability. Consequently the sector controller did not have a radar indication of the height of the Macchi. The coordination of a sector controller and an approach controller was hampered by the design of the management of the flight progress strip that is very crowded and difficult to read. That led the controller
Unaccomplished an after Take Off check list and distraction [12]	The checklist may not be completed within a time every time due to other tasks. If there is a delay in one task that affect remaining tasks and the performance and cognition of operators. The GPS setting task may distract the performance of operators. The aircraft was allowed to climb above 10,000 ft in an unpressurised state.
Unrecognising the cabin altitude warning system [12]	If an operator was captured in a task, the attention of his/her may not recognize the warning illumination because of distracted cognition of the operator.

Forgetting a conditional clearance of a taxiing aircraft to cross an active runway [13]	When a system did not provide any physical record, such as tactile memory markers) that a conditional clearance was pending, there was no cue to alert the controllers to the fact that this was the case. That led the aerodrome controller not to being aware that a conditional clearance was active when to clear EAL for take off.
Conducting a obscure V1 cut procedure at night [14]	When a procedure is not prohibiting firmly, it could be possible to conduct the procedure. The V1 cut procedure at daytime is permitted and there is not clear prohibition on the procedure at night. That led to the misinterpretation of the syllabus on the operation manual.
Unintentional actions in the controller-pilot data link communications (CPDLC) system [15]	If an operation is needed while conducting tasks, operators think the system provide the function, particularly, in computerized systems. The mouse buttons are easily to be entered without considerable considerations.
Not trusting in High frequency (HF) radio systems and relying on CPDLC[15]	The operator tends to rely on automated systems. That led operators not to using HF system relying on CPDLC.
Mismanagement of the fuel system [16]	The similarity of selection positions of switches on a system make human operators to error managing the system. That led the pilot making the mismanagement of fuel selection system.
Not follow rules of donning oxygen masks in an emergence condition [17]	There was no concrete and forced procedure to wear oxygen masks in case of a pressurization problem. Human operators tend to focus on a urgent task when they encounter an emergency. In this case, the urgent task is to avoid depressurization state of the aircraft. The pilots try to overcome the problem. That led to not wearing oxygen masks while their emergence works.
Confusion of flight progress strips in a flight progress strip system [18]	There was no additional space for the additional controllers in the console. The design of a flight progress strips positioning space and a procedure of positioning and disposition of strips is not enough for increased strips. In a busy traffic condition, busy space of flight progress strips cause a confusion or the omitting of flight progress for controllers. Just putting a person in the task would not help the operators
Confusion with capturing information in a traffic information transmission system [19]	When monitoring more than one frequency, the crews had to decide upon which frequency to maintain their primary focus in the face of competing cognitive demands. The design of the procedures used in the Demonstration Class G airspace did not fully consider the impact of radio congestion. That led the controller and the crew of King Air not correctly recognizing their transmissions.

Not noticing errors in Orion's navigation system [20]	The design of a procedure of the reconfiguration of a navigation system in the aircraft is based on a normal circumstance not high workload conditions. Navigation errors of a function of equipment limitations are not easily noticed by operators without any alert systems or procedure. That led the pilots not to notice navigation errors.
Unaccomplished check lists in a search plan [20]	The re-tasking note format does not provide any defence against the omission for key information. That led the pilot to forgetting checking the configuration of the navigation system.
Uncompleted a pre-flight check [21]	The difference between the pilot's operating manual and the operator's operations manual, and a comment of a manager to intend to delete the procedure made the pilot assuming no need to a balance check of fuel consumption.
Misunderstood a holding pattern procedure [22]	The Captain of the B767 reported that in the USA, where a holding pattern is not displayed, or in the absence of other information, a "default" right hand pattern is to be flown. There is no such procedure in Australia. As a result, the Captain elected to fly a right hand pattern without checking with air traffic control for holding pattern information. Without relevant information operators would follow previous experiences or general rules. That led the pilot make a wrong left turn instead of checking further information from the air traffic controller.
Confusing with marks in a terminal chart [22]	The depiction of the holding pattern was difficult to distinguish from other markings on the chart and the pattern was not displayed on the appropriate Standard Arrival Route (STAR) chart. In addition, the holding pattern was not loaded in the aircraft's flight management computer database. Difficult to distinguish against other information lead operators omitting information described in the chart.
Fail to conduct continuous monitoring of runway conditions [23]	The procedure for release of the runway from the aerodrome controller (ADC) to the SMC was for both the ADC and SMC to de-select their respective runway 11/29 selection buttons. Both buttons would became illuminated when selected on, indicating that the runway was active. To check an indication of the runway selector system is easier than to scan runways by eyes. That led the controller rely on the system not scanning runways.
Forgetting information during the air traffic instructions [23]	Eliminated data of flight progress strips easily pass away from operators' memory with other tasks.
Confusing with the airfield layout [23]	The threshold of runway 21 is at the midway point of runway 11/29 and access to the threshold of runway 21 was achieved by taxiing via runway 11. The airfield layout increased the potential for a runway incident. It is high workload crossing runways with many aircrafts landing and departing. That led the controllers fail to scan correctly runways.

Confusing with similar characters in a Sydney terminal chart [24]	The chart was ambiguous in that there was another letter "Y" displayed to the south of runway 25. That led the crew interpreted taxiway G3 to be taxiway Y on the basis of that information. The crew subsequently turned the aircraft onto taxiway G3, which was closed
Rely on one of fuel quantity assessment systems [25]	Pilots assume they can rely on the one of the two fuel quantity systems. That led to masking the unreliable fuel indicator and relying only on the fuel log system.
Rely on one of fuel quantity assessment system [26]	A fuel log system is not a direct assessment system causing errors. Checking fuel quantity by a dipstick is a difficult task and causing executing errors. That led pilots relying on fuel quantity gauges.
Trust in the computerised automatic terminal information system (CATIS) [27]	The controllers in the Adelaide Air Traffic Control tower had previously included information that the LLZ and the GP were not available on the computerised automatic terminal information system (CATIS) that is used to broadcast operational information to pilots. When the LLZ was returned for operational use, they abbreviated the advice to `localiser available', due to system constraints on the amount of additional information that could be included. The information that the GP was not available was not included in the CATIS. The majority of the additional information consisted of advice of restrictions due to aerodrome works. The CATIS was normally broadcast on the non-directional navigation beacon (NDB) and a very high frequency (VHF) radio transmitter. However, at the time of the occurrence the VHF transmitter was not available and the information was only available on the NDB. Despite listening to that information, the pilots missed the fact that the localiser was available due to the poor quality of the received audio. Consequently, when the pilots reported on first contact with the approach controller that they had received the CATIS they were unaware that only the localiser was available.
Distraction while conducting tasks in the controller pilot datalink and the sector 8 operating console [28]	The positioning of the controller pilot datalink and the sector 8 operating console restrict the ability of controllers to maintain an effective scan of the flight progress strip board. Controllers are required to divert their gaze and attention from the board to operate the controller pilot datalink keyboard.
Mismanagement of the position of the landing gear inhibit switch [29]	The switch was to be in the INHIBIT position, rendering the gear unable to extend. There was no indication of the position of INHIBIT switch. No caution advisories were illuminated. When the flight crew prepared the aircraft for flight, they did not confirm the position of the main landing gear inhibit switch.

Misinterpretation of a manual of a minimum equipment list (MEL) [30]	Part (b) of the Operations area of the operator's MEL stated: "(1) At low engine power (around idle thrust) setting: (a) Associated bleed is selected OFF…." The crew interpreted the operator's MEL to mean that at engine "idle thrust" they were to turn the bleed air from that engine to off. That prevented any supply of bleed air for the pressurisation and airconditioning system coming from that engine.
Not notice wires while conducting a flight[31]	The wires were aligned on 060 degrees magnetic, with a maximum height of 31.5 metres for the upper wire and 30.1 metres for the lower wire. The position of the wires was not annotated on the relevant Visual Terminal Charts and they did not have high visibility devices attached. A wire strike protection system (WSPS) had not been fitted to the helicopter. Company employees said that it was usual for the pilot to fly at a low height when transiting to and from the work location.
Misunderstood Reference terms [32]	The meaning of the term 'southern shores' was not available to the pilot of the Cessna and therefore the potential existed for the misunderstanding between the pilot and the aerodrome controller that resulted in this occurrence.
Mismanagement of emergency power lever (EPL) [33]	The POH did not address the engine control settings for training of this type, and the engine manufacturer's Service Information Letter (SIL) noted the use of the EPL for familiarization training, while suggesting that this training be completed on the ground. The discrepancy between these two documents may have led to the flight crew's belief that the use of the EPL for familiarization training in-flight was acceptable.
Not recognising incorrect data input into the multi-function control and display unit (MCDU) of the Flight management system (FMS) [34]	The sequence of FMS entries advised by the aircraft manufacturer provided an explanation of how the 2,500 ft step altitude, once removed, could have been incorrectly reinstated into the active flight plan. This meant that the FMS contained an incorrect step altitude for the inbound turn and that the automatic flight system would allow the aircraft to descend below the step altitude unless the crew intervened. The crew believed that they had operated the FMS system appropriately and were unaware that the constraint altitude had been changed. It is likely that they expected that the aircraft's automatic flight system would not infringe the vertical profile limits of the approach. However, it was apparent that they became distracted during the inbound turn by the track break or discontinuity on the map display.
Misunderstood the limitation of transponders of a Traffic Alert and Collision Avoidance System (TCAS) [35]	When had selected the transponder code and switched the unit to "On" prior to departing, the pilot assume its operation. They did not expect that the transponders could require up to five minutes warm-up prior to operation. The pilot was sure that the indicator light on the transponder was operating. The pilot did not believe that the transponder was not operating.

Rely on the Operational Data Information [36]	Coordination between the tower controllers and the Terminal Control Area controllers utilises the Operational Data Information contained within the radar label display. The use of Operational Data Information for coordination between units was accepted as a standard operating procedure. On some occasions the overuse and over reliance on Operational Data Information coordination may lead to a lack of situational awareness. Controllers were aware of what was intended to happen after the overshoot but there were no visual cues as to what the aircraft was doing. The approach and departures controllers coordinated via hotline for Departures to retain the Cessna on frequency and place the aircraft on a close right downwind. However there was no way for the aerodrome controller to know this unless the controller had queried the aircraft's current clearance. This may have led the approach controller to discount the Cessna from his mental traffic picture.
Rely on the fuel quantity indicating system [37]	A fuel log, if available, and a visual inspection of tank contents, if conducted, would have provided additional assurance regarding the quantity of fuel on board the aircraft. It is clear that the fuel gauges were not accurately indicating the quantity of fuel on board the aircraft, probably because of microbiological contamination. The pilot's method of establishing fuel on board was not robust, as it relied exclusively on the accuracy of the fuel quantity indicating system. In this context, the operations manual procedure was deficient in that it did not adequately address the individual fuel system characteristics of the different aircraft types in the operator fleet. However, the fuel system configuration of most aircraft in the operator's fleet, including the Nomad, meant that it was not possible to conduct a visual inspection of fuel quantity unless the fuel tanks were either full or nearly full. The pilot did not conduct a visual determination of fuel quantity, even though this was required by the operator's operations manual.
Unnoticed error in a data entry in Controller-Pilot Data Link Communications (CPDLC) [38]	Selection of a pre-formatted instruction and sending the message is a skill-based activity of easy of unintentional performance. In reply to the request by OEB for climb to FL330, the controller pre-selected the wrong pre-formatted CPDLC message and sent the message without checking it. The controller had not intended to assign FL330 to the crew of OEB and did not realise that they had been assigned FL330.
Misunderstood data in Weather Radar [39]	Due to the limitations of the airborne weather radar and possibly the radar antenna setting, the flight crew misinterpreted the depicted weather radar returns. The flight crew did not appear to understand the limitations of the airborne weather radar.
Unintentional data entry n Controller-Pilot Data Link Communications (CPDLC) [40]	The controller intended to send the message to the crew of the north-east bound B747 once they had passed the south-west bound B747 and a separation standard had been established. The controller had prepared a pre-formatted controller-pilot data link communication (CPDLC) message for transmission to the crew of the north-east bound B747. However, he unintentionally sent the message before the two aircraft had passed.

Monitoring the aircraft's weather radar [41]	When adverse weather condition is imminent, it is necessary the pilot in command was monitoring the aircraft's weather radar. The pilot became distracted while assessing the meteorological conditions. The distraction occurred as he monitored the weather radar and assessed the meteorological conditions that the aircraft was encountering during the climb.
Rely on cockpit displays [42]	The 737-400 cockpit displays did not have a similar indication because the altimeters are not connected to the FMC database that includes the aerodrome transition level/altitude information. The first officer's experience was primarily on the 737-400 and the pilot in command had primarily flown the newer 737-800, which was equipped with significantly more integrated and up-to-date cockpit displays compared with the 737-400. If the aircraft had been equipped with a similar display then the missed changeover from QNE to QNH may not have occurred.
Mismanagement of the calibrated dip stick [43]	The new fuel quantity check method for wooden dip stick differed from previous methods. He was not aware that this method for measuring the fuel quantity was only valid when using the original manufacturer's supplied dip stick. He had used the same technique to dip the fuel as he had been instructed to use with the original plastic dip stick. This technique could result in a significant over estimation of tank contents.
Failure of monitoring runways [44]	It is also likely that the white colour of Car 23 made it difficult to see against the background of white runway markings or white gable markers. Consequently, without an effective alert to the presence of the vehicle on the runway, the controller's scan was inadequate to see Car 23. The aerodrome controller did not change the 'runway designator' strip to indicate that Car 23 had entered the runway.
Failure of the blanket clearance [45]	The blanket clearance needs intensive cognitive loads for controllers. The presentation of the yellow flight progress strip did not alert the ADC that a runway 12/30 blanket clearance was in place. While conducting other task, it is possible the ADC and the SMC did not conduct an effective scan of runway 30 or the flight progress strip display prior to clearing the Pilatus to take off. They rely on each other.
Misidentification of morse-code in the flight management computer [46]	It is easy for human to make errors if a feature of an artefact in shape, colour, or number is similar. Both pilots incorrectly identified the morse-code ICN signal on frequency 109.5 MHz as ICS, the morse-code identifier for the runway 15 ILS on frequency 109.9 MHz. The pilot in command then incorrectly preset the manual frequency selector of his VHF navigation control panel to 109.5 MHz, the frequency for the runway 33 localiser at Cairns, morse-code identifier ICN.

Incomplete fuel consumption checks [47]	There was no logging of fuel usage for the helicopter that would have alerted the pilot to the greater than planned consumption rates. This meant significant differences between planned and actual fuel consumption rates remained undetected. The lack of any recorded fuel consumption checks meant that actual fuel consumption rates were not readily available to pilots flying the helicopter. The pilot did not check the actual fuel consumption.
An incomplete Weight check system [48]	As same task in everyday make people to conduct same pattern of the performance, it make easy to skip or ignore procedures/ factors that normally would have not be changed. When the agent who handled freight at Honolulu for the B767 operator received the pallet weights, she did not check the figures against the loadsheet issued by Load Control. Consequently, she did not realise that the weights stated on the loadsheet had already been converted to kilograms, and applied the conversion a second time. Also, as the agent for the US operator was confident that she had passed the correct weights to the B767 agent, she did not recheck to ensure that the B767 agent had received the correct weight information.
Misunderstanding of the emergency and abnormal checklist instructions [49]	The chief pilot's belief that emergency procedures learned during early training could be effectively applied to any general aviation aircraft did not allow for significant variations between aircraft systems and in particular fuel systems. The pilot's response to the engine failure was not consistent with the aircraft manufacturer's or the operator's emergency and abnormal checklist instructions.
Distraction while data entry into The Australian Advanced Air Traffic System (TAAATS) [50]	The controller then entered FL330 into TAAATS as the new cleared flight level (CFL). The controller reported that he had intended to confirm FL330 as the cleared flight level with the B767 crew at that time, but he unintentionally assigned FL300. The additional coordination and TAAATS entries associated with those aircraft that had been provided with a shorter track increased the controller's workload and may have distracted him as he was trying to assist them in their important task. It is also possible that the controller may not have detected the incorrect level assignment of FL300 because the level read back by the pilot phonologically matched the information stored in the controller's short-term memory; he may not have consciously processed the assigned flight level information in the read-back provided by the crew of the B767.
Mismanaging of the movement of a flap/slats and a landing gear lever [51]	The PIC immediately called for the flaps to be re-positioned, but the copilot selected the landing gear up. The actions of the copilot appear to have been an `action slip', a type of procedural error associated with two actions (landing gear and flaps/slats retraction) that are sequentially linked. As was the case here, in human behaviour there can sometimes be a `spill-over' that triggers the associated action at an inappropriate time. There may have been other inappropriate/inadvertent flap/slat selections in B717 aircraft.

Rely on the flight management system [52]	The pilot relies on the information provided by the flight management system. He did not pursue further checking from the air traffic controller.